David A. Green. Diverse Internet Experience as a Predictor for Online Privacy Concern. A Master's Paper for the M.S. in L.S degree. July, 2008. 73 pages. Advisor: Deborah Barreau

This study describes results of an online survey of students enrolled in the Graduate School at the University of North Carolina at Chapel Hill. The survey was conducted to assess the diversity of the students' Internet experience and how concerned they are with their online privacy.

People have different levels of concern about online privacy, and concern for privacy reflects in part the social, political, and cultural climate of a society at a point in time. It has been suggested that the extent and variety of online activities in which a user engages can be a good predictor of some kinds of Internet attitudes, including attitudes about information privacy. This study tests the hypothesis that users' concern with online privacy is related to users' diversity of experience on the Internet. The results showed no significant relationship between diverse Internet experience and overall online privacy concern. However, significant correlations were found for specific variables, such as the relationship between using the Internet for making calls and concern for government or service provider monitoring activity.

Headings:

Right of privacy

Internet/Security measures

Use Studies/Internet

Information retrieval/Social aspects

DIVERSE INTERNET EXPERIENCE AS A PREDICTOR FOR ONLINE PRIVACY CONCERN

by
David A. Green

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Library Science.

Chapel Hill, North Carolina

July 2008

Approved by

_____

Deborah Barreau

Table of Contents

Introduction

The Internet is a ubiquitous feature of daily life in the developed world. Advancements in technology and widespread use of the Internet have changed the way information about users is gathered, stored, and exchanged. While the changes may be blessings of convenience, the reality that our personal information is no longer restricted to our wallets and safes raises new concerns. Ours is an information society and entities within society can access, store, mine, buy, sell, analyze, and manipulate information about a user without that user even knowing it is happening. Every time we use the Internet we leave our digital footprint behind, allowing others to gather information about our lives, activities, and preferences. Just ask Amazon, Facebook, and eBay. Research in the area of online privacy concern has been stimulated by incidents of identity theft, increased prevalence of information technology throughout society, and media reports of government monitoring for homeland security.

Past research has identified a number of demographic and user-experience factors such as gender and length of Internet use that can affect user concerns about online privacy (Dommeyer & Gross, 2003; Graeff & Harmon, 2002; Milne & Rohm, 2000; O'Neil, 2001; Phelps, Nowak, & Ferrel, 2000; Sheehan, 1999) as well as social-psychological factors, such as people's beliefs and personality (Yao, Rice, & Wallis, 2007). Internet technology and the concept of privacy are both constantly evolving. It follows then that periodically monitoring users' privacy concerns may be useful. To

build upon this growing field, this study will analyze potential differences in privacy concerns among people with varying degrees of diversity of Internet use.

This paper addresses the following research question: Is there a relationship between people's Internet experience diversity and their online privacy concern? It is hypothesized that users with a broader range of experiences on the Internet will be less concerned with online privacy than those with less diverse experiences. For the purposes of this study, the population will be students enrolled in the Graduate School at the University of North Carolina at Chapel Hill. It is assumed that these students have had several years of experience with the Internet and thus will be able to answer all of the questions in the survey that will be used to gather data.

It is important to test factors that may affect users' concerns regarding privacy online. Doing so will allow us to determine ways to increase users' comfort with using the Internet for such convenient applications as shopping and banking. Determining the validity of users' comfort and improving safety (security checks, cookies, education, among others) are both needed. But revealing whether diversity of Internet use predicts a user's privacy concerns is integral in determining why a user feels safe.

By focusing solely on users' diversity of experience using the Internet, this study will explore implications for the field of personal online privacy. It intends to discern concerns among varying degrees of experienced users. If the hypothesis holds true, we will know experience breeds comfort, whether from confidence, knowledge or both. From there, we can make suggestions as to how to educate more concerned users in protecting their privacy. Such revelations would be helpful to researchers studying online privacy and may lend support to theories about the correlation between diversity

of experience and comfort using the Internet for tasks ranging from the mundane (e.g. surfing or downloading shareware) to the complex and sensitive (banking or shopping). Examples of entities who may consider the findings of this study useful include: scholars in information and library science, information technology professionals, librarians, ethics, privacy and intellectual property lawyers, webmasters and designers, data mining companies, and various other Internet companies. The results could be valuable to any user concerned with online privacy regarding what can be done to improve personal comfort while using the Internet.

Literature Review

This literature review is structured to first provide background and definitions relating to the topic: privacy, privacy concern, the history and future of the measurement of information privacy, privacy protection, and diversity of Internet use. Following these sections is a review of recent articles, arranged chronologically, that are particularly applicable to the present study. A summary will wrap up the literature review.

1.1 Privacy and Privacy Concern

There have been numerous attempts to determine a single, encompassing definition of the concept of privacy. One of the earliest still cited today, mostly in legal circles, is the right to be left alone (Cooley, 1880; Warren & Brandeis, 1890). In psychological literature, privacy is commonly associated with the right to prevent the disclosure of personal information to others (Westin, 1967; Altman, 1975). Other

definitions of privacy include matters that are personal and secretive (Stephen, 1967), the selective control of information (Bennett, 1967), an individual's ability to control personal information (Fried, 1970; Westin, 1967), or the degree of accessibility to an individual (Bok, 1984).

A more comprehensive way of defining the concept of privacy has emerged to be inclusive of the prior definitions. Burgoon, Parrott, LePoire, Kelley, Walther, and Perry (1989) introduced a multidimensional approach to define privacy as "the ability to control and limit *physical*, *interactional*, *psychological* and *informational* access to the self or one's group" (Burgoon et al., 1989, p. 132). A second of this kind from DeCew (1997) uses three dimensions: informational, accessibility and expressive privacy.

A crucial component of these dimensions is the desire to keep personal information safely away from others, i.e. privacy concern (Westin, 1967), and the ability to connect with others in a private manner. As such, the amount of privacy concern varies from individual to individual based on that person's own perceptions and values. The technology of the Internet complicates the issue further, challenging traditional definitions of privacy (Solove, 2004; Austin, 2003).

This paper will assume the multidimensional view of privacy, since it helps to overcome these challenges by illuminating more facets of privacy than earlier definitions and by allowing for dimensions to overlap. The Internet is a fluid, evolving entity; the characteristics that help define it should be as well. The multidimensional view of privacy creates that opportunity. For example, the dimension accessibility privacy overlaps with information privacy when the acquisition of information includes gaining access to an individual (DeCew, 1997). This combination is embodied in personal web

pages created on sites such as Facebook or MySpace: a page author decides what personal information the public can and cannot see, including facts that can lead a viewer directly to the author.

1.2 Measurement History and Future

In 1996, Smith, Milberg, and Burke designed the first measure for information privacy concerns. They called it the Concern for Information Privacy (CFIP) Scale and it measured individuals' concern regarding organizational practices. In it, four factors were identified as elements of an individual's concern for personal privacy: collection, errors, secondary use, and unauthorized access to information. Naturally, with advances in technology, research, and practice, the CFIP needs to be reevaluated. Methods of measuring online privacy will need reevaluation as long as online privacy has value in society and continues to be attacked. As such, many similar but revised scales have emerged since the CFIP was introduced in 1996.

The CFIP scale is an example of the many studies that tend to focus on informational privacy as a one-dimensional construct. To improve, it has been suggested that studies and surveys clearly separate out all of the different factors that can be considered as privacy issues (Harper & Singleton, 2001). Privacy is a multifaceted concept and thus the work studying it should reflect it by attempting to measure each factor.

Malhotra, Kim, and Agarwal (2004) introduced Internet Users Information Privacy Concerns (IUIPC). Recognizing that there are multiple aspects of information privacy, the authors identified key attitudes towards the following components of their

model: collection of personal information, control over this information, and awareness of privacy practices of companies gathering it. While the IUIPC did a better job of covering more aspects of informational privacy, it lacked the ability to test validity in different contexts, such as the type of information requested with which the respondents may be concerned and any rewards offered by marketers in exchange for that information (Phelps et al., 2000; Sheehan & Hoy, 2000).

And what about the potential benefits of a decrease in online privacy? The collection and storage of user information can breed personalized services, targeted suggestions, and an overall increase in convenience and efficiency. Potential benefit is a topic for which there is a lack of published findings. With practices such as storing credit card information and data mining becoming more commonplace, it may be necessary to create scales of measurement for users' views of the benefits of decreased informational privacy online.

As time has passed, the field of study in online privacy has expanded but also reached new and greater detail. Studies have suggested that people have well-established attitudes and concerns regarding their online privacy. Accordingly, their concerns could prompt users to take preventative measures. Discovering what these measures are and, more importantly, what effect they have on the resulting level of concern could be a vital component to understanding online informational privacy behaviors and attitudes. Paine et al. (2007) found that a significant portion of respondents reporting no concern stated as such because of actions they took to protect their privacy. The data suggest that it is not enough to simply question the level of concern. Research should also discern why the level is what it is by uncovering privacy-related behaviors.

1.3 Privacy Protection

There are four main theories of privacy protection: non-intrusion theory, seclusion theory, control theory, and limitation theory. Each theory attempts to define privacy risks more narrowly than can be found in the multifaceted and often incomplete (due to the nature of the ever-changing information landscape) definitions of the concept of privacy. A controversial issue with the current accepted definition of privacy is adversarial because it does not consider the environment and situational context, simply assuming people are vulnerable and that therefore all privacy risks are dangerous (Raab & Bennett, 1998).

It has been suggested that the privacy concept evolves as new avenues of privacy infringement surface and counters to them are created (Moor, 1997). Therefore, there is a need for an updated approach to studying privacy. Moor looks at normative privacy which specifically challenges the assumed vulnerability of people and proposes an alternative to privacy protection: control/restricted access theory. This theory considers the differences in people and the differences in their situation and assigns them levels of access accordingly.

Although both Moor (1997) and Raab and Bennett (1998) suggested a shift in study toward situational-defined online privacy attitudes and behavior, most research continues to regard online privacy concerns in the adversarial paradigm without situational context.

1.4 Diverse Internet Experience

Past studies have focused mainly on demographic factors affecting online privacy concerns of users or simply the magnitude of a certain population's concern. It has been suggested by Rice (2006) and Yao, Rice, and Wallis (2007) that the number of online activities participated in by a user can be a good predictor of some kinds of Internet attitudes. The practical knowledge and skills users derive from participation in online activities is their Diverse Internet Experience. This user characteristic should be more informative than simply the number of online activities or years using the Internet as it signifies familiarity with the Internet. One can imagine that an increase in familiarity could provide the tools to protect one's privacy or at least reduce anxiety. "The more people engage in diverse online activities and the greater fluency they have in Internet and Web features and activities, the better understanding they will have about advantages and potential threats associated with these activities" (Yao et al., 2007, p.712). Perhaps then, Diverse Internet Experience can predict the level of a user's online privacy concern.

1.5 Recent Empirical Research

Buchanan, Paine, and Joinson (2007) summarized the performance of three studies meant to create a valid measure of privacy concern, general caution, and technical protection. The researchers wanted to cover not only threats to informational privacy, but other personal aspects of privacy and related behaviors that are inherent in individuals. Each of these behaviors and privacy-related attitudes were analyzed from the results of a survey of 515 student volunteers (685 were invited) from Open University (OU) in the United Kingdom.

The Buchanan et al. study produced scales that have validity as online measures of privacy-related attitudes and behaviors. However, the authors suggested several ways the research could be improved, including: (1) ask more questions, (2) avoid bias by using phrasing less likely to bring out distrust, and (3) use a sample more proportional to the Internet population since OU students tend to be better educated, more likely to be female, and higher in socioeconomic status.

Questions from Buchanan et al.'s (2007) survey assigned significance to three important factors: general caution, technical protection, and privacy concern. For these factors, we have questions that can be used in future studies measuring online privacy. Buchanan and colleagues present some of the limitations of their research, which is useful for others designing their own surveys. Particularly, a significant number of questions must be asked and carefully presented in an unbiased manner.

Unlike Buchanan et al., Yao et al. (2007) created their own survey that presented over 400 undergraduate students at a southwestern U.S. university with a multitude of questions that could be answered on a scale of their attitudes or feelings towards certain stimuli. They also discussed topics including beliefs in privacy rights and how gender and Internet use experience relate to online privacy.

What makes the Yao et al. (2007) survey unique is that the questionnaire allowed participants to relate things that are more personal in nature than other online privacy surveys allow. For example, the authors asked about such simple variables as whether the respondents preferred tinted windows, needed time alone, or are uncomfortable in public restrooms. From the responses to these questions an all-encompassing view of the daily behavioral attitudes of the sample could be drawn. There are far more variables as

a result of this survey, but through much statistical analysis, the authors were able to find some interesting links between personal views and online privacy concerns.

In fact, one of the authors' major conclusions was that "future research on Internet privacy issues should consider the influence of individual differences," which would introduce considerations from fields of research in addition to information and library science: anthropology, psychology, sociology, communication, etc. The authors also determined that individuals' beliefs in privacy rights and the desire for privacy are the main factors influencing online privacy concern.

Some of the limitations of their study include the specific sample used and the fact that the data were self-reported. The authors suggested a form of data collection yet to be used in online privacy research: a quiz to determine participants' actual Internet expertise.

Rather than using a population solely comprised of students from one university, Paine et al. (2007) used a Dynamic Interviewing Programme to survey users of the instant messaging client ICQ to evaluate individuals' privacy concerns online and what, if any, action the individual may take to protect privacy. The purpose of the study was to go beyond typical past research, which focused mainly on the magnitude of concern, by looking at meanings of privacy online and determining users' specific concerns. The researchers sent the interview to 79,707 randomly selected ICQ users, from which 1,507 users responded. After data cleaning, in which all non-responses and unrelated or inappropriate responses were removed, 530 participants' responses were analyzed. About three quarters of the participants from the world round were male and the average age was 24.6 years.

The results of the Paine et al. (2007) study show that users are concerned with a wide variety of privacy issues and employ many techniques to protect themselves. Internet experience and age were found to be predictors of protection action and privacy concern, respectively. Because this survey was sent worldwide, participants' fluency in English is a concern when considering the validity of the study. As fewer than two percent of invitees completed the interview, the inherent privacy concerns of the people who participated in an online survey in the first place is likely to skew results.

Both the data collected and the method employed can inform future studies. From their study, we can see the most common concerns about privacy when online, actions taken to protect privacy, reasons for not having concerns or taking action, and what types of people they are. These results provide fodder for specific questions in future studies to target the most important issues. The researchers used an open ended question format, which allowed them to obtain a detailed understanding of users' attitudes and perceptions (Paine et al., 2007). On the other hand, the wide variety of responses created issues for grouping into similar clusters. The positives and negatives of such a question format must be considered when designing surveys.

Adding a new twist to the factors influencing online privacy behaviors and attitudes, Lauer and Deng (2007) evaluated the correlation between trust and perceived privacy. Since there are a number of factors that can influence users' perceptions of their relative level of privacy, the authors believe there is a strong connection with online trust. They point out that online trust can be crucial to the success or failure of businesses that use the Internet, in particular for transactions involving money.

The main purpose of the Lauer's and Deng's work is to test a trust model introduced in an Internet context (Mayer et al., 1995). A survey of 269 students from the business school of a large mid-western university in the United States was conducted. In the survey, two online privacy policies (created by the authors) are presented and data on the respondents' feelings toward them are recorded using a five-point Likert type scale. Viewpoints such as integrity, ability, trust, benevolence, customer loyalty, and customer willingness to provide truthful information are all evaluated.

First, and perhaps most importantly, Lauer and Deng concluded that the Mayer et al. (1995) model is reliable and no modifications to it are necessary. Generally, they also conclude that an information privacy policy does have an effect on a customer's perceived trustworthiness of the company. In turn, trust correlates with increased loyalty manifested in increased business and willingness to divulge more personal information. The authors' findings suggest that the privacy policy of a company has a significant influence on users' trust and therefore users' comfort in releasing personal information. The study also introduces heretofore unconsidered factors in the area of online privacy, namely: trustworthiness, loyalty, and truthfulness. Lauer and Deng suggest that these factors should be considered in this realm of research.

A limitation of the Lauer and Deng study comes from the sample itself. The authors point out that "while the student sample comes from a desirable customer demographic category (higher than average educational level and 20-35 year old age group), they may not be representative of a company's customers." Also, there is the simple matter of having them read the "company's" privacy policy, an uncommon practice of Internet users.

1.6 Summary

The concept of privacy is a complicated one whose definition may very well need to be altered and amended throughout time to account for changes in cultural attitudes and, more specifically to the issue of online privacy, technological advancements and innovations. The prevailing approach to understanding privacy is multidimensional, so that it may account for information control, accessibility, and the physical and expressive facets of privacy. Research into the concern for personal privacy has gained steam with the advent of the Internet and only continues as technology advances.

Due to the increased concern over online privacy, there is no shortage of research on this specific topic. The previous studies present some of the strengths and weaknesses of the produced research. Conducting a survey comprised of students from one university can limit the types of people who will respond, but should provide a more intimate knowledge of the population that can help in interpreting findings. On the other hand, a widely dispersed survey, as used by Paine et al. (2007) may have the opposite effect. Open ended questions reveal a greater range of responses but are difficult to evaluate. However, researchers were able to identify factors in online privacy perceptions, behaviors, and attitudes that need to be tested in future studies, perhaps in a style more similar to the one used by Buchanan et al. (2007). Close ended questions in a survey format can provide evidence which should make it easier to compare many variables.

Overwhelmingly, the studies beg for more research to be produced. Each one introduced new factors that need further inspection: privacy protection action, personal

predisposition for privacy concern, Internet use experience, and trust. Using the measurements of scale validated in past studies, future research can be done to determine exactly how significantly these factors influence Internet users' perceptions, attitudes, and behaviors concerning online privacy.

Methodology

To address the research question this study uses a survey, specifically in the form of an online questionnaire (Appendix A). The survey was composed of closed-ended questions. Aside from demographic questions regarding the respondents' age, gender, and school department, responses were recorded using the Likert Scale.

Survey research is ideal for addressing this study's research question as there is a need to collect original data to describe a population which would be too difficult to observe directly. Surveys are widely considered to be effective for measuring attitudes and behaviors, which is exactly the goal of this study. Surveys have the advantages of insuring standardized data format, quick and easy data collection, and simplified coding and analysis. Another reason for using the survey method is that it is relatively economical, particularly since it can be administered online. (Babbie, 2004)

Questionnaires can be used in many types of data collection, such as experiments or field research, but are mostly used in survey research. The questionnaire allows for an even simpler standardization process, which reduces time and costs while increasing the validity of the survey. Also on the topic of cost, a self-administered questionnaire is usually less expensive to conduct than other survey methods: a staff of only one person

can be sufficient to run the entire survey process. Finally, respondents are sometimes reluctant to answer, or at least answer honestly, questions of a sensitive nature in a face-to-face to interview. There is a better chance questions, such as those concerning controversial attitudes or deviant behaviors, will be answered candidly in an anonymous self-administered questionnaire. (Babbie, 2004)

There are drawbacks to a questionnaire, however. While it may be quicker and easier to perform, it can be more difficult to obtain a sample that is truly representative of the population. In addition, it is difficult, if not impossible, to ensure that the surveys will be completed or even responded to at all. In a questionnaire, it is best to avoid many complicated issues because there is no one there to explain any questions a respondent may have. Along the same lines, with no physical presence of those conducting a survey, no observations can be made aside from the responses to the already existing questions.

Within the questionnaire, only closed-ended questions will be used for this study. Responses to closed questions are more easily processed than responses for open-ended questions, in part because open-ended questions must be coded before analysis. As long as the questions and response options are clear and unambiguous, negative terms are avoided, and the instructions succinctly state the purpose, then understandable, closed-ended responses should yield greater uniformity. The questionnaire is exhaustive in its response categories; no respondents should ever feel a need to choose more than one answer or be unable to find the response they are seeking. When designing the closed-ended questions, the author made sure to create relevant and clear answers as failure to do so can skew results, a drawback of this type of question.

As mentioned earlier, survey research is advantageous as a method for collecting data economically. It also allows for a large amount of data to be collected and for a large population to be looked at from which to draw a sample. Typically, the standardization of data possible in survey research reduces the effort expensed in data collection, coding, and analysis. On the other hand, surveys are rather inflexible in that it is difficult, if not impossible, to change the survey in the middle of collection – one would probably have to start from scratch. Also, it is difficult to obtain an accurate view of social processes when people are taken out of their natural setting. Thus, survey research tends to be relatively weak in terms of validity, but strong in its reliability. (Babbie, 2004)

1.7 Subjects

The subject population of the study was students who attend the Graduate School of the University of North Carolina at Chapel Hill. This population provides a balance between having a diverse sample while still providing convenience to the administrator of the survey. There was no attempt to target students by gender, ethnicity, race, age, or academic interest and the population is diverse in these areas. The population was easily accessible through email to the author's colleagues at the same institution. However, any suggestions about the relationship being tested can only be applied to grad students at similar institutions.

Because of the voluntary nature of completing the survey, the invitation was sent out to the listservs of each program in the Graduate School. The listserv managers were contacted with an email including the IRB approved invitation to participate (Appendix

B), which they then sent out to their respective programs' students. The email invitation included a description of the study, Institutional Review Board approval information, and a link to the online questionnaire. The goal was for about 370 students to complete the survey. There was no exclusion or inclusion criteria.

The Graduate School population at UNC is consistently around 8,000 students. Using Salant and Dillman's (1994) table, for a population of 8,000 members there should be a sample of nearly 370 to make estimates with a sampling error of no more than +/- 5 percent, at the 95 percent confidence level.

Those willing to volunteer for participation were asked to click on the link embedded in the recruitment email, which would take them to the online questionnaire. The survey began with demographic questions about gender, age, and department name, and then presented questions about the respondents' confidence in their ability to perform specific tasks online followed by questions regarding their concerns with personal privacy online. The intent was for the survey to take no more than 10-15 minutes to complete, whereupon the subject was thanked for their participation.

The questionnaire was administered online using the Qualtrics software offered through the Odum Institute for Research in Social Science at UNC. The Odum Institute offers Qualtrics software free of charge to students for web survey data collection. During the collection of data, the Qualtrics software will monitor the survey progress and send updates and reminders. The data collected can be downloaded in various formats to view, such as .csv, SPSS, XML and HTML. There are also data analysis tools available with Qualtrics. (Odum Institute for Research in Social Science, 2007)

Results

1.8 Data Cleaning and Coding

Three hundred sixty-two surveys were received as a result of the invitation to participate. Of the 362 surveys recorded, eighteen were discarded because they were incomplete. Without responses to at least one of both the "Internet diversity" and the "online privacy concern" questions, data are useless to the study. The remaining response sets were downloaded from the Qualtrics survey website to the Statistical Package for the Social Sciences (SPSS) software program. As stated in the Methodology, most of the survey was composed of Likert scale response questions. For each response set, there was an option to choose "N/A." In coding the data set, all responses of "N/A" were removed and left as if the respondent had not answered the question at all.

Demographic variables (gender, age, and department) were coded individually. Responses to diversity of Internet experience (Questions 1-17, Appendix A) and online privacy (Question 18-28, Appendix A) concerns were coded individually, then re-coded to create two summary variables. While it is useful to look at how responses to individual questions correlate with one another (e.g. difficulty using Internet email vs. concern with receiving spam/junk email), the author wanted to see if general diversity of Internet experience correlates with general online privacy concern. Responses were grouped by taking the mean of the total score for all questions in each group to create a summated scale. The result was the creation of two new variables: Diverse Internet Experience and Online Privacy Concern.

1.9 Testing the New Variables

Cronbach's coefficient alpha was used to compute the internal consistency reliability of the new variables. This computation gives an estimation based on the average correlation among variables comprising the set. Cronbach's alpha ranges from zero to one, with one indicating a perfect consistency, with no error component. At first run, the new variable Diverse Internet Experience had a Cronbach's alpha of .849, while Online Privacy Concern had a Cronbach's alpha of .896. However, testing needed to be done to confirm that each item belonged within these new variables.

To assess the reliability of each item within these new variables, each question was individually tested in two ways. The first test for the usefulness of the new variables checked the corrected item-total correlation, which is the Pearsonian correlation of each item with the total of scores on all other items. A low item-total correlation means the item has little correlation with the summary variable. An acceptable correlation is .40 or higher, showing that it is at least moderately correlated with the other items and will make a good component of a summated rating scale (Leech, Barrett, & Morgan, 2008). A negative correlation indicates the need to recode the item in the opposite direction. For the variable Diverse Internet Experience, Questions 1-7 each had too low of an item-total correlation. Sometimes, the removal of one item can affect the item-total correlation of another item to the point that a previously successful item is rendered useless or brings one that was too low back to an acceptable level (Leech, Barrett, & Morgan, 2008). The removal of any of Questions 1-7 or any possible combination of these questions did not benefit the other items nor did it significantly lower any of Questions 8-17 item-total correlation. Thus, all of Questions 1-7 were permanently removed from the new variable

Diverse Internet Experience. For the variable Online Privacy Concern, all questions had an acceptable item-total correlation, and thus none were removed.

The second test checked for significant improvement of Cronbach's alpha if an item was deleted. After testing the item-total correlation and removing Questions 1-7, Diverse Internet Experience's new Cronbach's alpha was .912 (Table 1), so the purging of items improved the reliability of this new variable.

Table 1.
Diverse Internet Experience

Reliability Statistics

Cronbach's Alpha	N of Items
.912	10

Table 2.
Online Privacy Concern

Reliability Statistics

Cronbach's Alpha	N of Items
.896	11

For the second test, the removal of only one question would raise Cronbach's alpha for Diverse Internet Experience, but only by .004, so it was kept (Appendix C, 1). As for Online Privacy Concern (Table 2), the removal of the question regarding the receipt of spam or junk email is the only one that would improve its Cronbach's alpha of .896, and by only .001 (Appendix C, 4). Thus, no more items needed to be removed from these new variables. Diverse Internet Experience is now a description of scores from Questions 8-17 and Online Privacy Concern from Questions 18-28.

1.10 Demographic Data

Three questions were used to gather demographic data about the respondents to the survey. The purpose was to gather the gender, age, and department in which each was enrolled. Of the 344 respondents used for this study, 214 (62.2%) were female and 128 (37.2%) were male (Table 3). Two respondents did not answer the gender question.

Table 3.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	214	62.2	62.6	62.6
	Male	128	37.2	37.4	100.0
	Total	342	99.4	100.0	
Missing	System	2	.6		
Total		344	100.0		

In the latest data from The University of North Carolina at Chapel Hill, 59.6% of the total 2007 Fall semester enrollees were women and 40.4% were men (UNC Office of the Registrar, 2008). The mean age of respondents was 27.7 years, ranging from 15 to 54 years of age (Appendix C, 9). Over 69% were among the ages of 23-28. Respondents were spread out among the departments of the Graduate School (Appendix C, 10). Nearly a quarter of them were from the School of Information and Library Science, however. The next largest representation was from the Department of Chemistry at 9.7% of the total respondents.

1.11 Diverse Internet Experience Correlation with Online Privacy Concern

The Pearson Product Moment Correlation (r) was used to assess the association or relationship between variables in the study. More commonly known as the Pearson correlation coefficient, this is a bivariate parametric statistic, a measure of linear association between two variables. The significance level (or p-value) is the probability of obtaining results as extreme as the one observed. If the significance level is very small (less than 0.05) then the correlation is significant. If the significance level is relatively large (for example, 0.50) then the correlation is not significant and the two variables are

not linearly related. In all of the correlation tables, one asterisk (*) signifies that the correlation is statistically significant at the 0.05 level. Two asterisks (**) signifies that the correlation is statistically significant at the 0.01 level.

The new variables, Diverse Internet Experience and Online Privacy Concern, had their possible correlation assessed with the Pearson correlation coefficient and no statistical significance was found (Table 4). Thus, we cannot accept the null hypothesis of this study that users from this population with a broader range of experiences on the Internet will be less concerned with online privacy than those with less diverse experiences. The correlations table displays Pearson correlation coefficients, significance values, and the number of cases with non-missing values.

Table 4.

Correlations

		Experience	Concern
Experience	Pearson Correlation	1	.025
	Sig. (2-tailed)		.657
	N	340	322
Concern	Pearson Correlation	.025	1
	Sig. (2-tailed)	.657	
	N	322	323

1.12 Other Correlations

There was still the possibility that individual experiences and skills correlated with individual items of concern. Also, there could be statistically significant correlations between each of the summation scale variables and the individual items. Finally, gender and age could be tested against Diverse Internet Experience and Online Privacy Concern. Thus, correlations were drawn for every possible combination of these variables, resulting in 219 tests (17 experience items for each of the 11 concern items, 11

correlations with Diverse Internet Experience, 17 items correlations with Online Privacy Concerns, 4 for gender and age). There were many statistically significant correlations. But, the correlations are small and not linearly related (see Appendix C, 12), which makes it difficult to state definite suggestions about the relationships between these variables.

Tables 5-18 illustrate significant correlations between variables.

Table 5.

Correlations

		Experience	Internet service provider monitoring email or any other online activity
Experience	Pearson Correlation	1	.120*
	Sig. (2-tailed)		.034
	N	340	316
Internet service provider monitoring email or any other online activity	Pearson Correlation	.120*	1
	Sig. (2-tailed)	.034	
	N	316	317

*. Correlation is significant at the 0.05 level (2-tailed).

Table 6.

Correlations

		Use Internet email	Receiving spam/junk email
Use Internet email	Pearson Correlation	1	.139*
	Sig. (2-tailed)		.013
	N	343	318
Receiving spam/junk email	Pearson Correlation	.139*	1
	Sig. (2-tailed)	.013	
	N	318	319

*. Correlation is significant at the 0.05 level (2-tailed).

Table 7.

Correlations

		Finding a privacy certification on a web site before registering your information	Internet service provider selling personal information	Internet service provider monitoring email or any other online activity
Finding a privacy certification on a web site before registering your information	Pearson Correlatio	1	.131*	.136*
	Sig. (2-tailed)		.024	.019
	N	311	300	301
Internet service provid selling personal information	Pearson Correlatio	.131*	1	.743**
	Sig. (2-tailed)	.024		.000
	N	300	316	313
Internet service provid monitoring email or an other online activity	Pearson Correlatio	.136*	.743**	1
	Sig. (2-tailed)	.019	.000	
	N	301	313	317

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 8.

Correlations

		Use advanced search techniques with a search engine	Hacker obtaining personal medical information online
Use advanced search techniques with a search engine	Pearson Correlation	1	.112*
	Sig. (2-tailed)		.049
	N	335	310
Hacker obtaining personal medical information online	Pearson Correlation	.112*	1
	Sig. (2-tailed)	.049	
	N	310	318

*. Correlation is significant at the 0.05 level (2-tailed).

Table 9.

Correlations

		Checking a computer for spyware	Internet service provider monitoring email or any other online activity	Government monitoring email or any other online activity
Checking a computer for spyware	Pearson Correlatio	1	.113*	.164**
	Sig. (2-tailed)		.048	.004
	N	318	307	310
Internet service provi monitoring email or a other online activity	Pearson Correlatio	.113*	1	.615**
	Sig. (2-tailed)	.048		.000
	N	307	317	315
Government monitori email or any other online activity	Pearson Correlatio	.164**	.615**	1
	Sig. (2-tailed)	.004	.000	
	N	310	315	320

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 10.

Correlations

		Changing cookie preferences	Attack of a computer virus
Changing cookie preferences	Pearson Correlation	1	-.140*
	Sig. (2-tailed)		.015
	N	326	304
Attack of a computer viru	Pearson Correlation	-.140*	1
	Sig. (2-tailed)	.015	
	N	304	319

*. Correlation is significant at the 0.05 level (2-tailed).

Table 11.

Correlations

		Making a phone call online	Internet service provider monitoring email or any other online activity	Internet service provider selling personal information
Making a phone call online	Pearson Correlatio	1	.151*	.128*
	Sig. (2-tailed)		.017	.042
	N	270	252	253
Internet service provi monitoring email or a other online activity	Pearson Correlatio	.151*	1	.743**
	Sig. (2-tailed)	.017		.000
	N	252	317	313
Internet service provi selling personal information	Pearson Correlatio	.128*	.743**	1
	Sig. (2-tailed)	.042	.000	
	N	253	313	316

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 12.

Correlations

		Chatting online	Hacker obtaining personal medical information online
Chatting online	Pearson Correlation	1	-.117*
	Sig. (2-tailed)		.043
	N	324	302
Hacker obtaining personal medical information online	Pearson Correlation	-.117*	1
	Sig. (2-tailed)	.043	
	N	302	318

*. Correlation is significant at the 0.05 level (2-tailed).

Table 13.

Correlations

		Turn on or off auto loaded images	Government monitoring email or any other online activity	Receiving spam/junk email
Turn on or off auto loaded images	Pearson Correlat	1	-.152*	.129*
	Sig. (2-tailed)		.016	.041
	N	271	251	250
Government monitor email or any other online activity	Pearson Correlat	-.152*	1	.194**
	Sig. (2-tailed)	.016		.001
	N	251	320	318
Receiving spam/junk email	Pearson Correlat	.129*	.194**	1
	Sig. (2-tailed)	.041	.001	
	N	250	318	319

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Table 14.

Correlations

		Clearing your browser history	Internet service provider monitoring email or any other online activity
Clearing your browser history	Pearson Correlation	1	.120*
	Sig. (2-tailed)		.034
	N	326	314
Internet service provide monitoring email or any other online activity	Pearson Correlation	.120*	1
	Sig. (2-tailed)	.034	
	N	314	317

*. Correlation is significant at the 0.05 level (2-tailed).

Table 15.

Correlations

		Determine who is responsible for maintaining a website you are viewing	Attack of a computer virus	Government monitoring email or any other online activity
Determine who is responsible for maintaining a website you are viewing	Pearson Correlati	1	.183**	-.154**
	Sig. (2-tailed)		.002	.009
	N	312	288	289
Attack of a computer	Pearson Correlati	.183**	1	.224**
	Sig. (2-tailed)	.002		.000
	N	288	319	316
Government monitori email or any other onl activity	Pearson Correlati	-.154**	.224**	1
	Sig. (2-tailed)	.009	.000	
	N	289	316	320

**. Correlation is significant at the 0.01 level (2-tailed).

Table 16.

Correlations

		Blocking messages or emails from someone	Government monitoring email or any other online activity
Blocking messages or emails from someone	Pearson Correlation	1	.135*
	Sig. (2-tailed)		.019
	N	309	301
Government monitorin email or any other online activity	Pearson Correlation	.135*	1
	Sig. (2-tailed)	.019	
	N	301	320

*. Correlation is significant at the 0.05 level (2-tailed).

Table 17.

Correlations

		et browser t accept or eject cookies	Hacker obtaining personal medical information online	Attack of a computer virus	Government monitoring email or any other online activity	Receiving spam/junk email
Set browser to acce reject cookies	Pearson Correla	1	.124*	.139*	-.129*	.115*
	Sig. (2-tailed)		.031	.016	.026	.046
	N	326	301	302	302	301
Hacker obtaining personal medical information online	Pearson Correla	.124*	1	.359**	.353**	.262**
	Sig. (2-tailed)	.031		.000	.000	.000
	N	301	318	315	315	314
Attack of a compute	Pearson Correla	.139*	.359**	1	.224**	.378**
	Sig. (2-tailed)	.016	.000		.000	.000
	N	302	315	319	316	315
Government monito email or any other c activity	Pearson Correla	-.129*	.353**	.224**	1	.194**
	Sig. (2-tailed)	.026	.000	.000		.001
	N	302	315	316	320	318
Receiving spam/jur email	Pearson Correla	.115*	.262**	.378**	.194**	1
	Sig. (2-tailed)	.046	.000	.000	.001	
	N	301	314	315	318	319

*·Correlation is significant at the 0.05 level (2-tailed).

**·Correlation is significant at the 0.01 level (2-tailed).

Table 18.

Correlations

		Gender	Experience	Concern
Gender	Pearson Correlation	1	.180**	-.124*
	Sig. (2-tailed)		.001	.026
	N	342	338	322
Experience	Pearson Correlation	.180**	1	.025
	Sig. (2-tailed)	.001		.657
	N	338	340	322
Concern	Pearson Correlation	-.124*	.025	1
	Sig. (2-tailed)	.026	.657	
	N	322	322	323

**· Correlation is significant at the 0.01 level (2-tailed).

*· Correlation is significant at the 0.05 level (2-tailed).

Discussion

The present study was conducted to examine a possible relationship between people's Internet experience diversity and their online privacy concerns. It was hypothesized that users with a broader range of experience on the Internet will be less concerned with online privacy than those with less diverse experiences. The population studied was students enrolled in the Graduate School at the University of North Carolina at Chapel Hill. The results suggest that individuals' general Internet experience diversity does not correlate with their concerns with online privacy within this population. However, the results do suggest that certain experiences can affect online privacy concerns.

1.13 Diverse Internet Experience and Online Privacy Concern

There are several possible explanations for why the results from this study failed to support the hypothesis that Internet use diversity directly affects online privacy concern. Of course, it could be that the Internet use diversity of this population's individuals truly does not influence concerns about online privacy. The population itself is far less diverse than one would find in society as a whole. The respondents are students seeking advanced degrees at a nationally ranked school. Thus, their level of education and experiences using the Internet are not as varied as the rest of society, and much of their Internet use occurs in an environment where academic freedom and openness are valued. But it could also be that the more time spent online performing various tasks leads to exposure to more threats than a novice user would encounter. The increase in comfort from experience then may be balanced out by the increased chance of

invasion of privacy. Further, an expert Internet user may be aware of more online privacy threats than a novice user. Following the *ignorance is bliss* credo, expert users may have an increased level of online privacy concern because of their greater awareness of danger. Future research should examine the experiences and awareness of users in more detail to classify their knowledge more accurately.

1.14 Individual Item Correlations

In creating the summation scale variables Diverse Internet Experience and Online Privacy Concern to generalize respondents' characteristics, seven questions were thrown out of consideration. These questions were discarded to improve the internal consistency reliability of the new variables; however, it does not mean the responses to these questions are useless. Also, it is possible that by grouping the other ten Internet experience diversity questions together, some experiences were submerged within the new scale without being given their due attention. The same attention should be paid to the individual privacy concerns, as well. Therefore, correlations were tested between all experience items and concern items. For further interest, gender and age were correlated with experience items and concern items. Certain significant correlations make intuitive sense (Table 19).

However, some correlations are more difficult to explain. One such correlation is between confidence in turning auto loaded images on or off and concern about receiving spam or junk email. Displaying auto loaded images on a web browser or email message will not by itself cause spam or junk mail to be sent to a user. However, it could be that the respondents consider the presence of auto loaded images will increase the chance they

will click on a link that could bring about spam mail. Another explanation could be that the respondents believe emails can contain auto-loaded images. But, these assumptions would be inferences on behavior and technological knowledge that is not specifically evaluated in the questions.

Table 19.

Experience Item	Concern Item
Use Internet email	Receiving spam/junk email
Finding a privacy certification on a web site before registering personal information	Internet service provider monitoring email or any other online activity
	Internet service provider selling personal information
Cookie preferences	Attack of a computer virus
	Hacker obtaining personal medical information
	Government monitoring email or any other online activity
	Receiving spam/junk email
Clearing browser history	Internet service providers monitoring email or any other online activity
Determine who is responsible for a website that is being viewed	Attack of a computer virus
Making a phone call online	Internet service provider monitoring email or any other online activity
	Internet service provider selling personal information
Checking a computer for spyware	Internet service provider monitoring email or any other online activity
	Government monitoring email or any other online activity

In future research, more explicit questions should be asked to tab exactly why Internet users behave the way they do, or qualitative methods should be used to elicit information about motives. The purpose of the summary variables was to overcome the limitations of assessing all possible specific questions. By creating a summation scale of

the respondents' characteristics regarding Internet use diversity and online privacy concern, the study attempted to lump all of those variables together to generalize experience as it relates to concern. Because the results did not support the hypothesis, it is possible that the questions were inadequate or perhaps even inappropriate. As stated earlier, it is also possible that diverse Internet experience does not influence online privacy concern.

1.15 Limitations of the Study

As discussed earlier, questions are more likely to be answered candidly in an anonymous self-administered questionnaire than other forms of surveying. Still, it is not without its limitations. The invitation to participate was sent via email and the survey itself was completed online. People who are comfortable with technology and unconcerned about privacy are more likely to respond than those who are not due to the nature of the distribution of the survey. For this reason and because the administrator has little control of the sample, while an online questionnaire may be quicker and easier to perform, it can be more difficult to obtain a sample that is truly representative of the population.

This study is also limited in that the population is students of the Graduate School at the University of North Carolina at Chapel Hill. We can make suggestions regarding the behaviors and concerns of only these students from the results. Further research should be done for a wider population, including a greater age range, larger geographical coverage, and various levels of education. Doing so would cover a wider array of concerns and experience levels. A more accurate summation of Internet users is needed

to better comprehend and evaluate the relation between diversity of Internet experience and online privacy concerns.

Conclusion

The concept of privacy continues to develop as cultural attitudes evolve, privacy is invaded in new ways, and protection systems are created. To keep up with evolving social standards, researchers must persistently update approaches to studying privacy. The current approach to understanding and defining privacy is multidimensional, which includes information control, accessibility, and the physical and expressive components of privacy. To keep pace with the progressing technological landscape, techniques for measuring privacy concern have matured with the need to take on the many dimensions of online privacy.

Paine et al. (2007) found that a significant portion of respondents with no online concern attributed their lack of concern to personal actions taken to protect their privacy. It has been suggested by Rice (2006) and Yao et al. (2007) that the number of online activities participated in by a user can be a good predictor of some kinds of Internet attitudes. These findings led to the present study addressing the following research question: Is there a relationship between people's Internet experience diversity and their online privacy concern? Data was gathered through a survey of 362 students enrolled in the Graduate School at the University of North Carolina at Chapel Hill.

The results of this study did not show a significant correlation between an individual's diversity of Internet experience and their online privacy concern. There

were some statistically significant correlations between specific experiences and concerns, but the correlations were small and not linearly related. The study's findings suggest that future research should gather data from a more diverse population to increase the variance of Internet users' characteristics. It would also be useful to ask more detailed questions to first pinpoint which Internet experiences influence online privacy concern before tackling the broader approach attempted in this study. Online privacy research has room for much growth, and new studies will hopefully shed further light on the reasons for Internet users' concerns.

Bibliography

Altman, I. (1975). *The environment and social behavior*. Brooks/Cole, Monterey, CA.

Austin, L. (2003). Privacy and the question of technology. *Law and Philosophy, 22*, 119-166.

Babbie, E. (2004). *The practice of social research* (10th ed.). Belmont, CA: Wadsworth/Thomson Learning.

Bennett, C. (1967). What price privacy. *American Psychologist, 22,* 371-376.

Bok, S. (1984). *Secrets: on the ethics of concealment and revelation*. New York: Oxford University Press.

Buchanan, T., Paine, C., & Joinson, A.N. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58* (2), 157-165.

Burgoon, J.K., Parrott, R., LePoire, B.A., Kelley, D.L., Walther, J.B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships, 6,* 131-158.

Cooley, T. (1880). *A treatise on the law of torts or the wrongs which arise independent of contract*. Chicago: Callaghan.

DeCew, J. (1997). *In pursuit of privacy: law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

Dommeyer, C.J., & Gross, B.L. (2003). What consumers know and what they do: an investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing, 17*, 34-51.

Fried, C. (1970). *An anatomy of values: problems of personal and social choice*. Cambridge, MA: Harvard University Press.

Graeff, T.R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing, 19*, 302-313.

Harper, J., & Singleton, S. (2001). With a grain of salt: what consumer privacy surveys don't tell us. *Competitive Enterprise Institute*.

Lauer, T.W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security, 6* (5), 323-331.

Leech, N.L., Barrett, K.C., & Morgan, G.A. (2008). *SPSS for intermediate statistics: use and interpretation*. New York: L. Erlbaum Associates.

Malhotra, N.K., Kim, S.S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale and a causal model. *Information Systems Research, 15* (4), 336-355.

Mayer, R.C., Davis, J.H, & Schoorman, F.D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20* (3), 709-734.

Milne, G.R., & Rohm, A.J. (2000). Consumer privacy and name removal across direct marketing channels: exploring opt-in and opt-out alternatives. *Journal of Public Policy and Marketing, 19,* 238-249.

Moor, J.H. (1997). Towards a theory of privacy in the information age. *Computers and Society*, *27* (3), 27-32.

Odum Institute for Research in Social Science. (2007). Web survey data collection. In *Data Collection Services*. Retrieved November 12, 2007, from http://www.irss.unc.edu/odum/jsp/content_node.jsp?nodeid=362#OwnWeb

Office of Institutional Research & Assessment. (2007). Fall 2007 headcount enrollment. In *Enrollment and Student Characteristics*. Retrieved November 12, 2007, from http://oira.unc.edu/facts-and-figures/student-data/enrollment-and-student-characteristics.html

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review*, 19, 17-31.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A.N., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65* (6), 526-536.

Phelps, J.E., Nowak, G.J., & Ferrel, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*, 27-41.

Raab, C.D., & Bennett, C.J. (1998). The distribution of privacy risks: who needs protection? *The Information Society*, *14* (4), 263-74.

Rice, R.E. (2006). Influences, usage, and outcomes of Internet health information searching: multivariate results from the Pew surveys. *International Journal of Medical Informatics*, *75* (1), 8-28.

Salant, P., & Dillman, D. A. (1994). *How to conduct your own survey*. New York, NY: John Wiley & Sons.

Sheehan, K.B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 13* (4), 24-38.

Sheehan, K.B., & Goy, M.G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy Marketing, 19* (1), 62-73.

Smith, J.H., Milberg, S.J., & Burke, S.J. (1996). Information privacy: measuring individuals concerns about organizational practices. *MIS Quarterly, 20*, 167-196.

Solove, D.J. (2004). *The digital person: technology and privacy in the information age*. NYU Press.

Stephen, J.F. (1967). *Liberty, equality, fraternity*. Indianapolis, IN: Liberty Fund, Inc.

UNC Office of the Registrar. (2008). Student counts by registration type. In *Frequently Requested Reports*. Retrieved June 26, 2008, from http://regweb.unc.edu/stats/reports/cntqk079.html

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4,* 193-220.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Yao, M.Z., Rice, R.E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology, 58* (5), 710-722.

Appendix A – Online Questionnaire

My name is David Green, and I am a graduate student at the School of Information and Library Science at the University of North Carolina at Chapel Hill. The following is a research study to collect data for my Master's paper. The study is about online privacy concerns as they relate to the diversity of experiences using the Internet. The results of this study will help determine how to better educate Internet users to protect their privacy.

The study will require 5 to 10 minutes of your time and is completely voluntary. If you wish to participate in the study, just click below to proceed to the survey. The study is completely anonymous and no further contact will be made. This research has been approved by the Institutional Review Board at UNC-CH (IRB Study 08-0511).

This study is conducted under the supervision of Dr. Deborah Barreau (barreau@ils.unc.edu). Please contact me at dagreen@unc.edu if you have any questions.

Demographic Data

We would like to know just a little about you so we can see how different types of people feel about the issues we will be examining (please indicate the correct response).

Gender:

○ Female

○ Male

What is your age: _____

In which department at UNC are you a student?

(Drop-down box)

Internet diversity

Please indicate the degree to which you find it difficult to perform the following tasks while using the Internet on a scale of 1 (very easy) to 7 (very difficult). Please select N/A if you have never tried to perform the task because there never was a need for you to do so.

1. Use a browser to navigate the web

   1 2 3 4 5 6 7 N/A

2. Use Internet email

   1 2 3 4 5 6 7 N/A

3. Use a search engine

   1 2 3 4 5 6 7 N/A

4. Use advanced search techniques with a search engine

   1 2 3 4 5 6 7 N/A

5. Turn on or off auto loaded images

   1 2 3 4 5 6 7 N/A

6. Set browser to accept or reject cookies

   1 2 3 4 5 6 7 N/A

7. Determine who is responsible for maintaining a website you are visiting

   1 2 3 4 5 6 7 N/A

Please indicate the level of confidence you have in your ability to perform the following actions on a scale of 1(not confident at all) to 7 (very confident).

8. Making an online order purchase

   1 2 3 4 5 6 7 N/A

9. Changing cookie preferences

   1 2 3 4 5 6 7 N/A

10. Chatting online

    1 2 3 4 5 6 7 N/A

11. Making a phone call online

    1 2 3 4 5 6 7 N/A

12. Using a pop up window blocker

    1 2 3 4 5 6 7 N/A

13. Checking a computer for spyware

    1 2 3 4 5 6 7 N/A

14. Clearing your browser history

    1 2 3 4 5 6 7 N/A

15. Reading a license agreement fully before agreeing to it

    1 2 3 4 5 6 7 N/A

16. Finding a privacy certification on a web site before registering your information

    1 2 3 4 5 6 7 N/A

17. Blocking messages or emails from someone

    1 2 3 4 5 6 7 N/A

Online privacy concerns

Please indicate the degree to which you are concerned with the following items on a scale of 1 (not concerned at all) to 7 (very concerned):

18. Hacker obtaining credit card information online

    1 2 3 4 5 6 7 N/A

19. Hacker obtaining personal medical information online

    1 2 3 4 5 6 7 N/A

20. Hacker obtaining other personal information online

    1 2 3 4 5 6 7 N/A

21. Attack of a computer virus

    1 2 3 4 5 6 7 N/A

22. Internet service provider selling personal information

    1 2 3 4 5 6 7 N/A

23. Internet service provider monitoring email or any other online activity

    1 2 3 4 5 6 7 N/A

24. Government monitoring email or any other online activity

    1 2 3 4 5 6 7 N/A

25. Employer/university monitoring email or any other online activity

    1 2 3 4 5 6 7 N/A

26. Receiving spam/junk email

    1 2 3 4 5 6 7 N/A

27. Online organizations not being who they claim to be

1 2 3 4 5 6 7 N/A

28. People online not being who they claim to be

1 2 3 4 5 6 7 N/A

We thank you for your time spent taking this survey.

Your response has been recorded.

Appendix B – Email Invitation to Participate in Study

Dear fellow graduate students,

My name is David Green, and I am a graduate student at the School of Information and Library Science at the University of North Carolina at Chapel Hill. I am writing to invite you to participate in a research study to collect data for my Master's paper. The study is about online privacy concerns as they relate to the diversity of experiences using the Internet. The results of this study will help determine how to better educate Internet users to protect their privacy. The study will require 5 to 10 minutes of your time and is completely voluntary.

The questionnaire can be found online at http://uncodum.qualtrics.com/SE?SID=SV_a8WvevyAJgpXMEc&SVID=Prod. If you wish to participate in the study, just click the link and you will be on your way. The study is completely anonymous and no contact beyond this email will be made. This research has been approved by the Institutional Review Board at UNC-CH (IRB Study 08-0511).

This study is conducted under the supervision of Dr. Deborah Barreau (barreau@ils.unc.edu). Please contact me at dagreen@unc.edu if you have any questions.

Survey link:
http://uncodum.qualtrics.com/SE?SID=SV_a8WvevyAJgpXMEc&SVID=Prod

Sincerely,
David Green
School of Information and Library Science
UNC Chapel Hill
dagreen@unc.edu

Appendix C – Tables, Histograms, and Scatter Plots

(1) Reliability test of Diverse Internet Experience

Case Processing Summary

		N	%
Cases	Valid	227	66.0
	Excluded[a]	117	34.0
	Total	344	100.0

a. Listwise deletion based on all variables in the procedure.

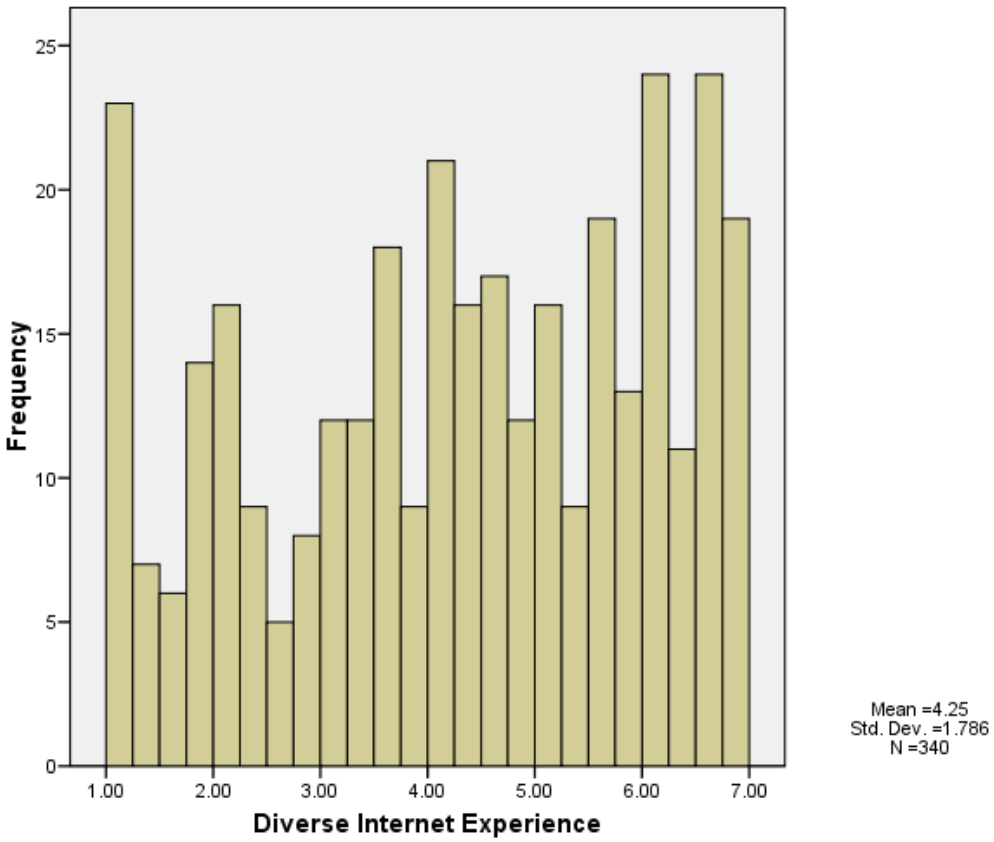
Reliability Statistics

Cronbach's Alpha	N of Items
.912	10

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Making an online order purchase	40.05	224.542	.724	.901
Changing cookie preferences	40.72	231.487	.810	.895
Chatting online	40.31	224.189	.776	.897
Making a phone call online	41.00	243.965	.608	.907
Using a pop up window blocker	40.48	227.056	.828	.894
Checking a computer for spyware	40.69	242.303	.651	.905
Clearing your browser history	39.99	231.040	.773	.897
Reading a license agreement fully before agreeing to it	40.82	253.677	.451	.916
Finding a privacy certification on a web site before registering your information	41.22	255.633	.516	.912
Blocking messages or emails from someone	40.56	242.407	.651	.905

(2) Histogram of Diverse Internet Experience frequency



(3) Frequencies for items within Diverse Internet Experience

Making an online order purchase

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	123	35.8	36.4	36.4
	2	13	3.8	3.8	40.2
	3	3	.9	.9	41.1
	4	1	.3	.3	41.4
	6	26	7.6	7.7	49.1
	7	172	50.0	50.9	100.0
	Total	338	98.3	100.0	
Missing	System	6	1.7		
Total		344	100.0		

Changing cookie preferences

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	57	16.6	17.5	17.5
	2	44	12.8	13.5	31.0
	3	41	11.9	12.6	43.6
	4	33	9.6	10.1	53.7
	5	35	10.2	10.7	64.4
	6	47	13.7	14.4	78.8
	7	69	20.1	21.2	100.0
	Total	326	94.8	100.0	
Missing	System	18	5.2		
Total		344	100.0		

Chatting online

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	108	31.4	33.3	33.3
	2	18	5.2	5.6	38.9
	3	10	2.9	3.1	42.0
	4	5	1.5	1.5	43.5
	5	15	4.4	4.6	48.1
	6	41	11.9	12.7	60.8
	7	127	36.9	39.2	100.0
	Total	324	94.2	100.0	
Missing	System	20	5.8		
Total		344	100.0		

Making a phone call online

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	59	17.2	21.9	21.9
	2	33	9.6	12.2	34.1
	3	30	8.7	11.1	45.2
	4	25	7.3	9.3	54.4
	5	36	10.5	13.3	67.8
	6	36	10.5	13.3	81.1
	7	51	14.8	18.9	100.0
	Total	270	78.5	100.0	
Missing	System	74	21.5		
Total		344	100.0		

Using a pop up window blocker

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	78	22.7	23.1	23.1
	2	40	11.6	11.9	35.0
	3	15	4.4	4.5	39.5
	4	25	7.3	7.4	46.9
	5	35	10.2	10.4	57.3
	6	47	13.7	13.9	71.2
	7	97	28.2	28.8	100.0
	Total	337	98.0	100.0	
Missing	System	7	2.0		
Total		344	100.0		

Checking a computer for spyware

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	55	16.0	17.3	17.3
	2	32	9.3	10.1	27.4
	3	33	9.6	10.4	37.7
	4	46	13.4	14.5	52.2
	5	38	11.0	11.9	64.2
	6	43	12.5	13.5	77.7
	7	71	20.6	22.3	100.0
	Total	318	92.4	100.0	
Missing	System	26	7.6		
Total		344	100.0		

Clearing your browser history

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	61	17.7	18.7	18.7
	2	17	4.9	5.2	23.9
	3	21	6.1	6.4	30.4
	4	18	5.2	5.5	35.9
	5	26	7.6	8.0	43.9
	6	34	9.9	10.4	54.3
	7	149	43.3	45.7	100.0
	Total	326	94.8	100.0	
Missing	System	18	5.2		
Total		344	100.0		

Reading a license agreement fully before agreeing to it

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	52	15.1	16.4	16.4
	2	34	9.9	10.7	27.0
	3	39	11.3	12.3	39.3
	4	40	11.6	12.6	51.9
	5	36	10.5	11.3	63.2
	6	31	9.0	9.7	73.0
	7	86	25.0	27.0	100.0
	Total	318	92.4	100.0	
Missing	System	26	7.6		
Total		344	100.0		

Finding a privacy certification on a web site before registering your information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	30	8.7	9.6	9.6
	2	60	17.4	19.3	28.9
	3	48	14.0	15.4	44.4
	4	46	13.4	14.8	59.2
	5	52	15.1	16.7	75.9
	6	33	9.6	10.6	86.5
	7	42	12.2	13.5	100.0
	Total	311	90.4	100.0	
Missing	System	33	9.6		
Total		344	100.0		

Blocking messages or emails from someone

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	42	12.2	13.6	13.6
	2	36	10.5	11.7	25.2
	3	29	8.4	9.4	34.6
	4	29	8.4	9.4	44.0
	5	46	13.4	14.9	58.9
	6	41	11.9	13.3	72.2
	7	86	25.0	27.8	100.0
	Total	309	89.8	100.0	
Missing	System	35	10.2		
Total		344	100.0		

(4) Reliability test of Online Privacy Concern

Case Processing Summary

		N	%
Cases	Valid	296	86.0
	Excluded[a]	48	14.0
	Total	344	100.0

a. Listwise deletion based on all variables in the procedure.

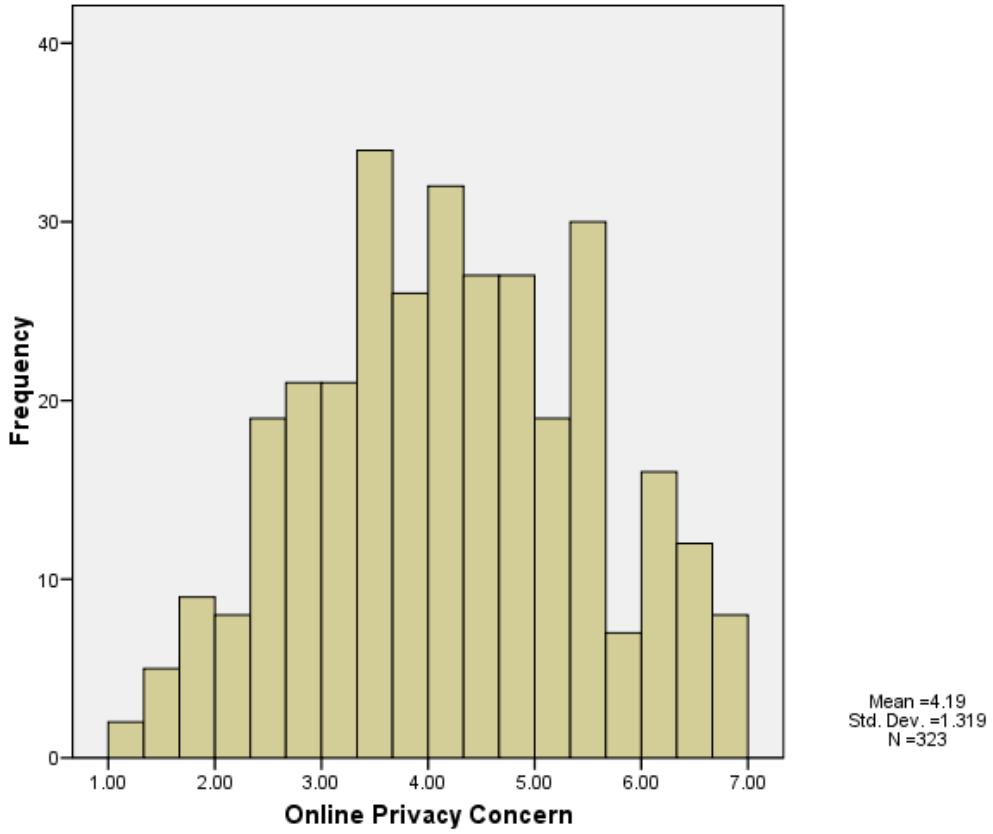
Reliability Statistics

Cronbach's Alpha	N of Items
.896	11

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Hacker obtaining credit card information online	42.07	167.235	.696	.883
Hacker obtaining personal medical information online	43.22	167.711	.634	.886
Hacker obtaining other personal information online	42.23	165.472	.723	.881
Attack of a computer virus	41.98	175.705	.486	.894
Internet service provider selling personal information	42.24	164.937	.660	.884
Internet service provider monitoring email or any other online activity	42.27	164.654	.657	.885
Government monitoring email or any other online activity	42.55	165.143	.589	.889
Employer/university monitoring email or any other online activity	42.50	164.142	.662	.884
Receiving spam/junk email	41.92	175.329	.439	.897
Online organizations not being who they claim to be	42.32	163.703	.718	.881
People online not being who they claim to be	42.56	166.118	.627	.887

(5) Histogram of Online Privacy Concern frequency



(6) Frequencies for items within Online Privacy Concern

Hacker obtaining personal medical information online

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	57	16.6	17.9	17.9
	2	73	21.2	23.0	40.9
	3	56	16.3	17.6	58.5
	4	48	14.0	15.1	73.6
	5	40	11.6	12.6	86.2
	6	21	6.1	6.6	92.8
	7	23	6.7	7.2	100.0
	Total	318	92.4	100.0	
Missing	System	26	7.6		
Total		344	100.0		

Hacker obtaining other personal information online

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	17	4.9	5.3	5.3
	2	49	14.2	15.3	20.6
	3	39	11.3	12.1	32.7
	4	66	19.2	20.6	53.3
	5	59	17.2	18.4	71.7
	6	52	15.1	16.2	87.9
	7	39	11.3	12.1	100.0
	Total	321	93.3	100.0	
Missing	System	23	6.7		
Total		344	100.0		

Attack of a computer virus

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	13	3.8	4.1	4.1
	2	35	10.2	11.0	15.0
	3	49	14.2	15.4	30.4
	4	37	10.8	11.6	42.0
	5	68	19.8	21.3	63.3
	6	76	22.1	23.8	87.1
	7	41	11.9	12.9	100.0
	Total	319	92.7	100.0	
Missing	System	25	7.3		
Total		344	100.0		

Internet service provider selling personal information

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	27	7.8	8.5	8.5
	2	46	13.4	14.6	23.1
	3	39	11.3	12.3	35.4
	4	39	11.3	12.3	47.8
	5	67	19.5	21.2	69.0
	6	51	14.8	16.1	85.1
	7	47	13.7	14.9	100.0
	Total	316	91.9	100.0	
Missing	System	28	8.1		
Total		344	100.0		

Internet service provider monitoring email or any other online activity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	28	8.1	8.8	8.8
	2	47	13.7	14.8	23.7
	3	38	11.0	12.0	35.6
	4	43	12.5	13.6	49.2
	5	61	17.7	19.2	68.5
	6	48	14.0	15.1	83.6
	7	52	15.1	16.4	100.0
	Total	317	92.2	100.0	
Missing	System	27	7.8		
Total		344	100.0		

Government monitoring email or any other online activity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	45	13.1	14.1	14.1
	2	62	18.0	19.4	33.4
	3	30	8.7	9.4	42.8
	4	41	11.9	12.8	55.6
	5	43	12.5	13.4	69.1
	6	49	14.2	15.3	84.4
	7	50	14.5	15.6	100.0
	Total	320	93.0	100.0	
Missing	System	24	7.0		
Total		344	100.0		

Employer/university monitoring email or any other online activity

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	36	10.5	11.2	11.2
	2	58	16.9	18.1	29.3
	3	35	10.2	10.9	40.2
	4	44	12.8	13.7	53.9
	5	66	19.2	20.6	74.5
	6	41	11.9	12.8	87.2
	7	41	11.9	12.8	100.0
	Total	321	93.3	100.0	
Missing	System	23	6.7		
Total		344	100.0		

Receiving spam/junk email

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	20	5.8	6.3	6.3
	2	36	10.5	11.3	17.6
	3	35	10.2	11.0	28.5
	4	45	13.1	14.1	42.6
	5	56	16.3	17.6	60.2
	6	63	18.3	19.7	79.9
	7	64	18.6	20.1	100.0
	Total	319	92.7	100.0	
Missing	System	25	7.3		
Total		344	100.0		

Online organizations not being who they claim to be

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	25	7.3	7.8	7.8
	2	46	13.4	14.4	22.3
	3	41	11.9	12.9	35.1
	4	58	16.9	18.2	53.3
	5	51	14.8	16.0	69.3
	6	60	17.4	18.8	88.1
	7	38	11.0	11.9	100.0
	Total	319	92.7	100.0	
Missing	System	25	7.3		
Total		344	100.0		

People online not being who they claim to be

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	42	12.2	13.3	13.3
	2	42	12.2	13.3	26.7
	3	39	11.3	12.4	39.0
	4	63	18.3	20.0	59.0
	5	41	11.9	13.0	72.1
	6	51	14.8	16.2	88.3
	7	37	10.8	11.7	100.0
	Total	315	91.6	100.0	
Missing	System	29	8.4		
Total		344	100.0		

(7) Demographic statistics

Statistics

		Gender	Age	Department
N	Valid	342	343	341
	Missing	2	1	3
Mean		1.37	27.70	22.79
Median		1.00	27.00	24.00
Mode		1	27	24
Std. Deviation		.485	5.475	13.327
Variance		.235	29.971	177.604

(8) Gender frequencies

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	214	62.2	62.6	62.6
	Male	128	37.2	37.4	100.0
	Total	342	99.4	100.0	
Missing	System	2	.6		
Total		344	100.0		

(9) Age frequencies

Age

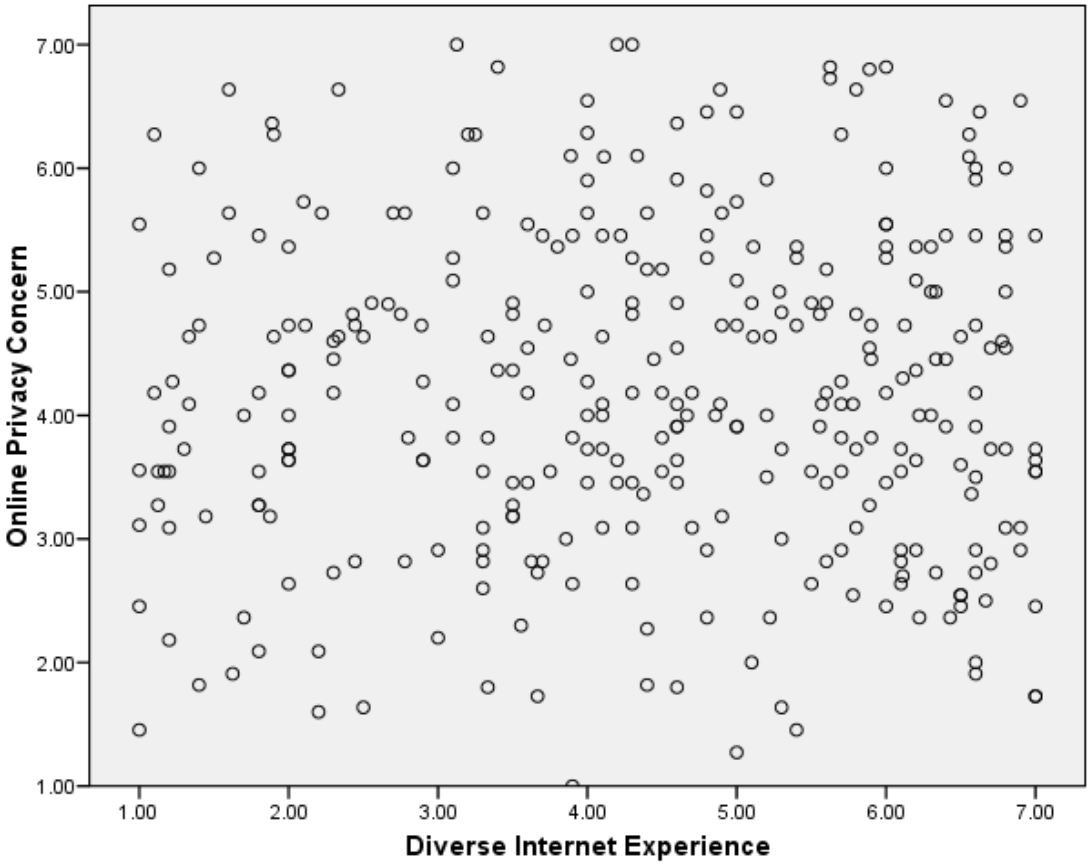
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	15	1	.3	.3	.3
	21	1	.3	.3	.6
	22	15	4.4	4.4	5.0
	23	42	12.2	12.2	17.2
	24	31	9.0	9.0	26.2
	25	44	12.8	12.8	39.1
	26	35	10.2	10.2	49.3
	27	45	13.1	13.1	62.4
	28	40	11.6	11.7	74.1
	29	21	6.1	6.1	80.2
	30	11	3.2	3.2	83.4
	31	7	2.0	2.0	85.4
	32	6	1.7	1.7	87.2
	33	5	1.5	1.5	88.6
	34	6	1.7	1.7	90.4
	35	4	1.2	1.2	91.5
	36	2	.6	.6	92.1
	37	4	1.2	1.2	93.3
	38	3	.9	.9	94.2
	39	2	.6	.6	94.8
	40	6	1.7	1.7	96.5
	41	1	.3	.3	96.8
	43	1	.3	.3	97.1
	44	1	.3	.3	97.4
	46	2	.6	.6	98.0
	47	1	.3	.3	98.3
	48	1	.3	.3	98.5
	49	2	.6	.6	99.1
	50	1	.3	.3	99.4
	54	2	.6	.6	100.0
	Total	343	99.7	100.0	
Missing	System	1	.3		
Total		344	100.0		

(10) Department frequencies

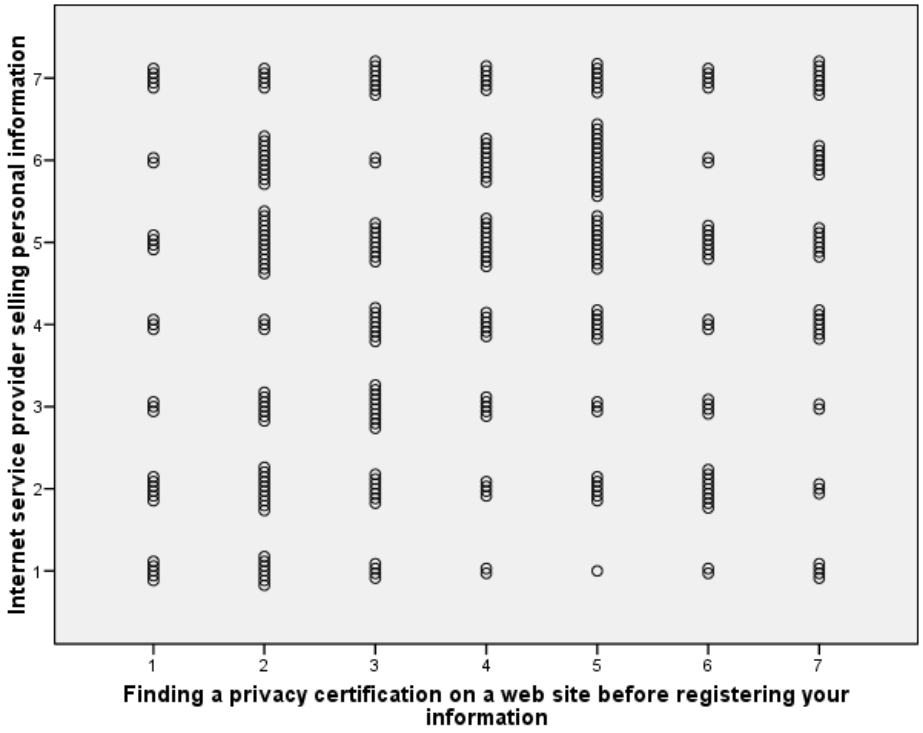
Department

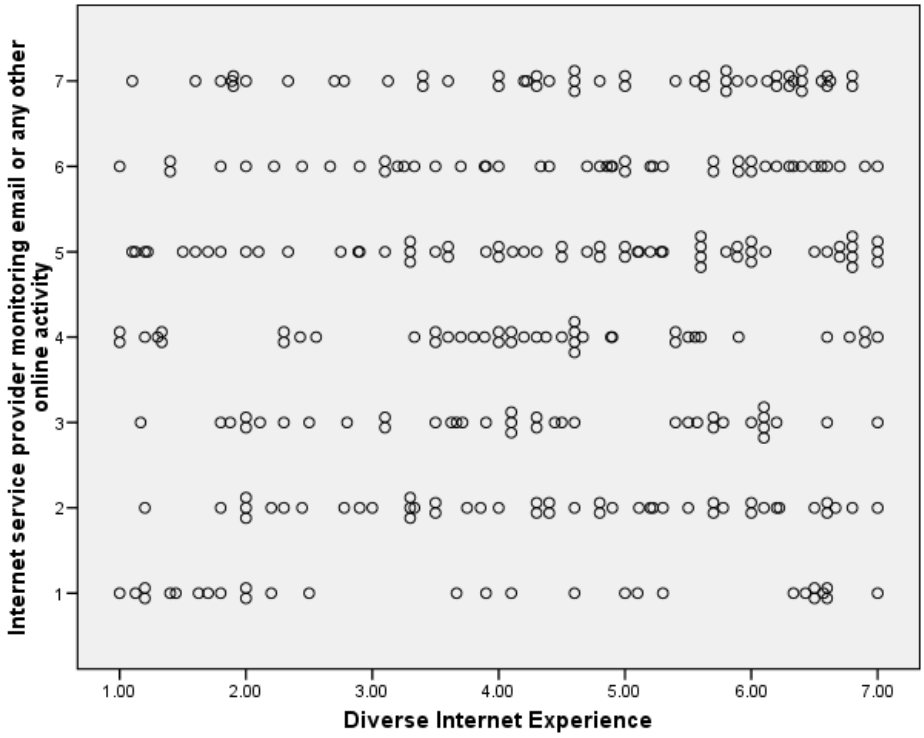
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Anthropology	6	1.7	1.8	1.8
	Art	4	1.2	1.2	2.9
	Chemistry	33	9.6	9.7	12.6
	City & Regional Planning	18	5.2	5.3	17.9
	Classics	4	1.2	1.2	19.1
	Communication Studies	8	2.3	2.3	21.4
	Comparative Literature	2	.6	.6	22.0
	Computer Science	16	4.7	4.7	26.7
	Dramatic Art	2	.6	.6	27.3
	Ecology	3	.9	.9	28.2
	Economics	9	2.6	2.6	30.8
	English	12	3.5	3.5	34.3
	Environmental Sciences & Engineering	1	.3	.3	34.6
	Exercise & Sport Science	10	2.9	2.9	37.5
	History	13	3.8	3.8	41.3
	Information & Library Science	83	24.1	24.3	65.7
	Journalism & Mass Communication	10	2.9	2.9	68.6
	Marine Sciences	2	.6	.6	69.2
	Mathematics	4	1.2	1.2	70.4
	Nutrition	16	4.7	4.7	75.1
	Philosophy	3	.9	.9	76.0
	Political Science	3	.9	.9	76.8
	Psychology	16	4.7	4.7	81.5
	Public Administration	10	2.9	2.9	84.5
	Public Policy	4	1.2	1.2	85.6
	Religious Studies	10	2.9	2.9	88.6
	Romance Languages	4	1.2	1.2	89.7
	Social Work	21	6.1	6.2	95.9
	Sociology	14	4.1	4.1	100.0
	Total	341	99.1	100.0	
Missing	System	3	.9		
Total		344	100.0		

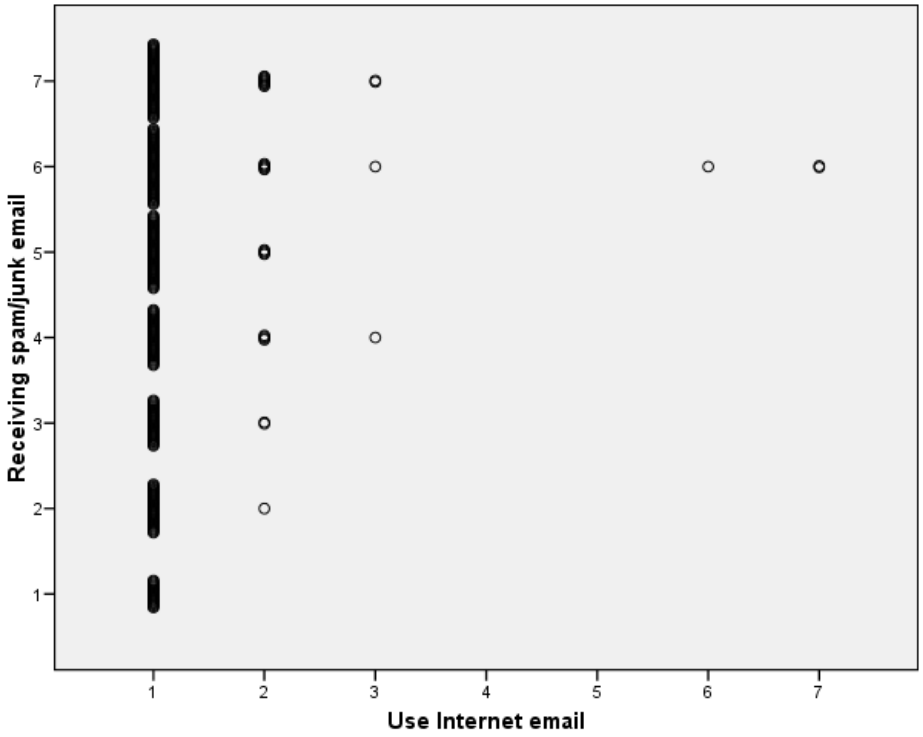
(11) Scatterplot of correlation between Diverse Internet Experience and Online Privacy Concern

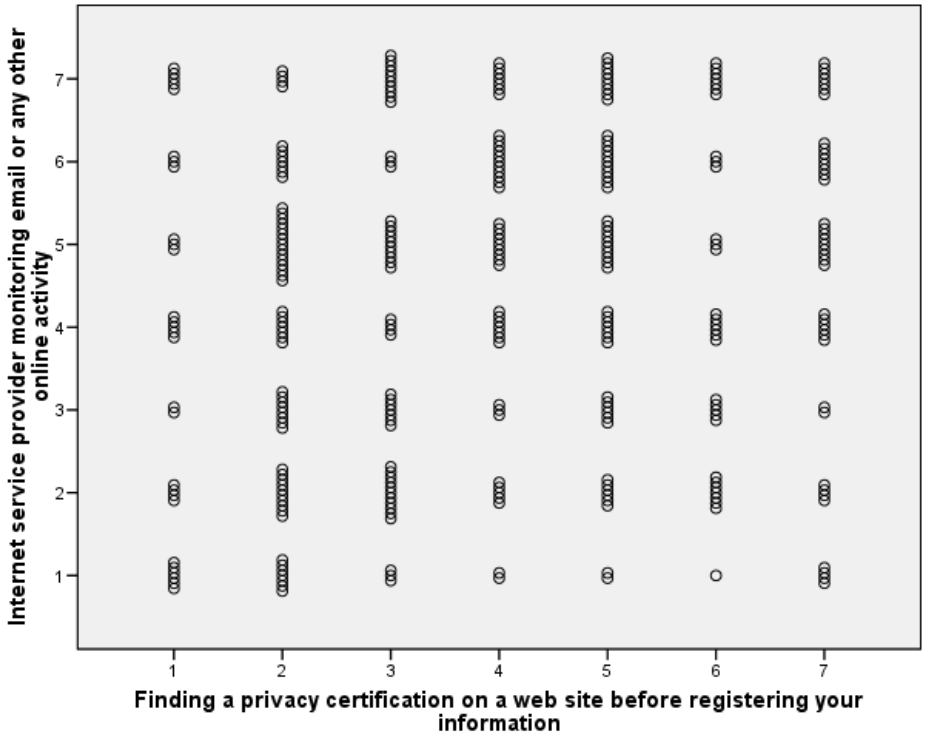


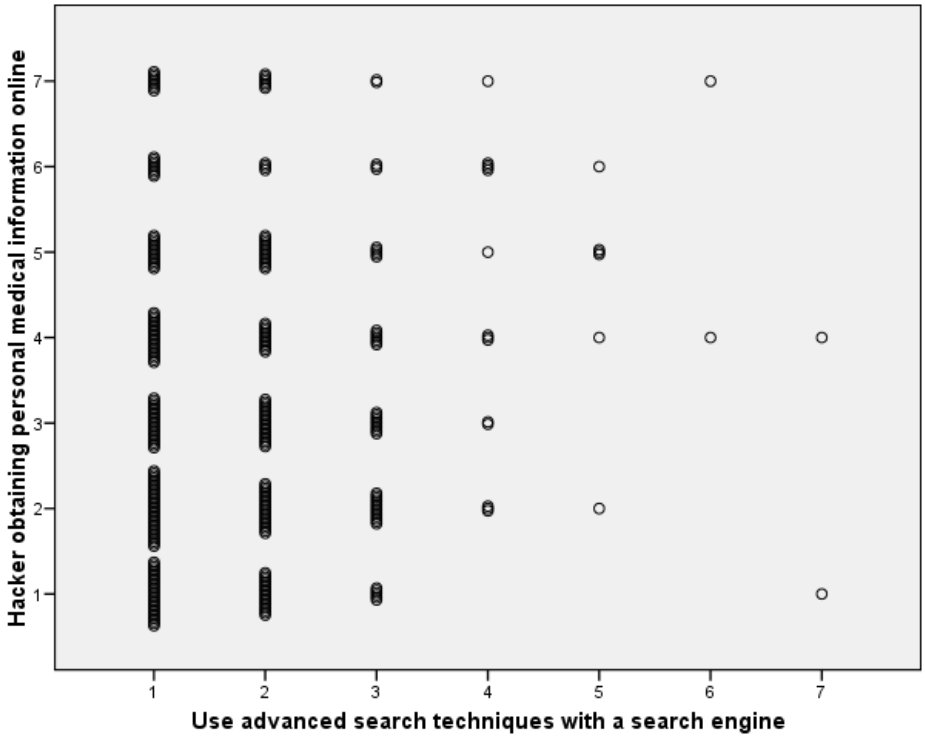
(12) Scatterplots of statistically significant correlations with stacked identical values

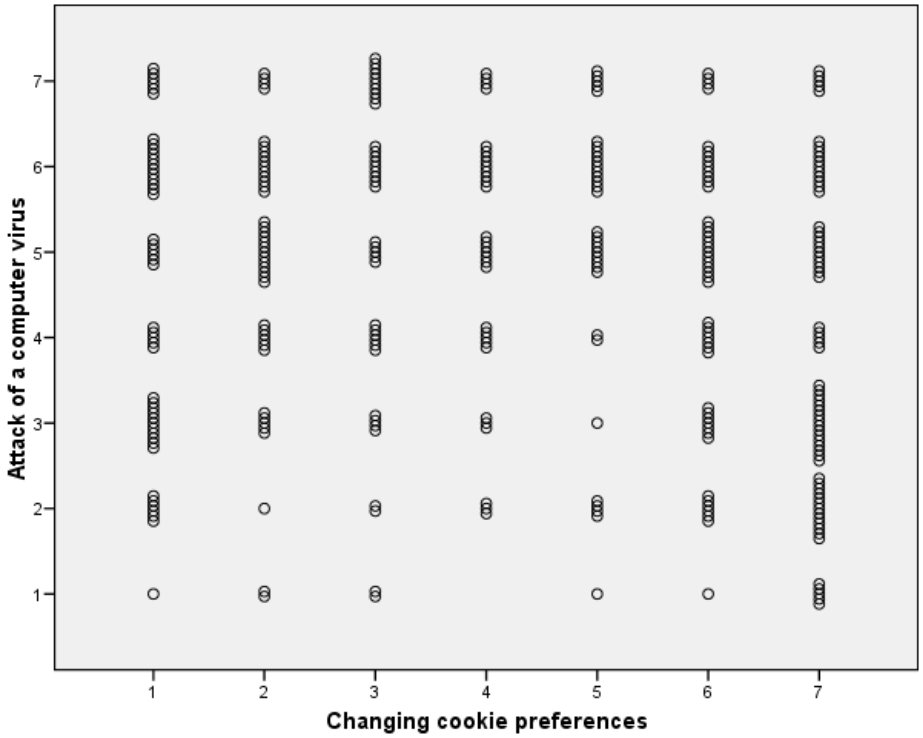


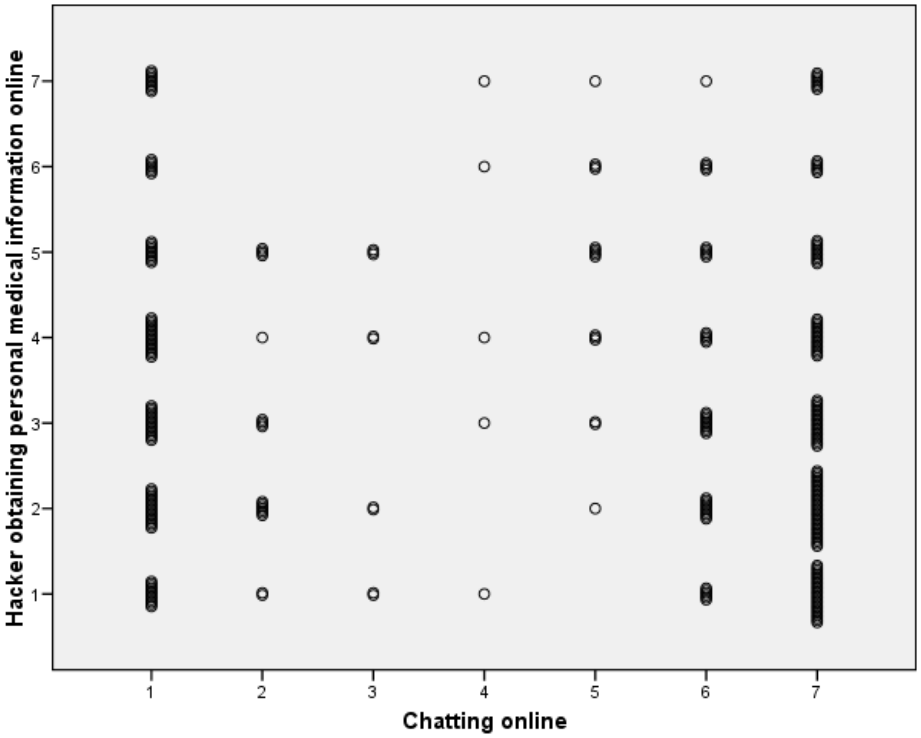


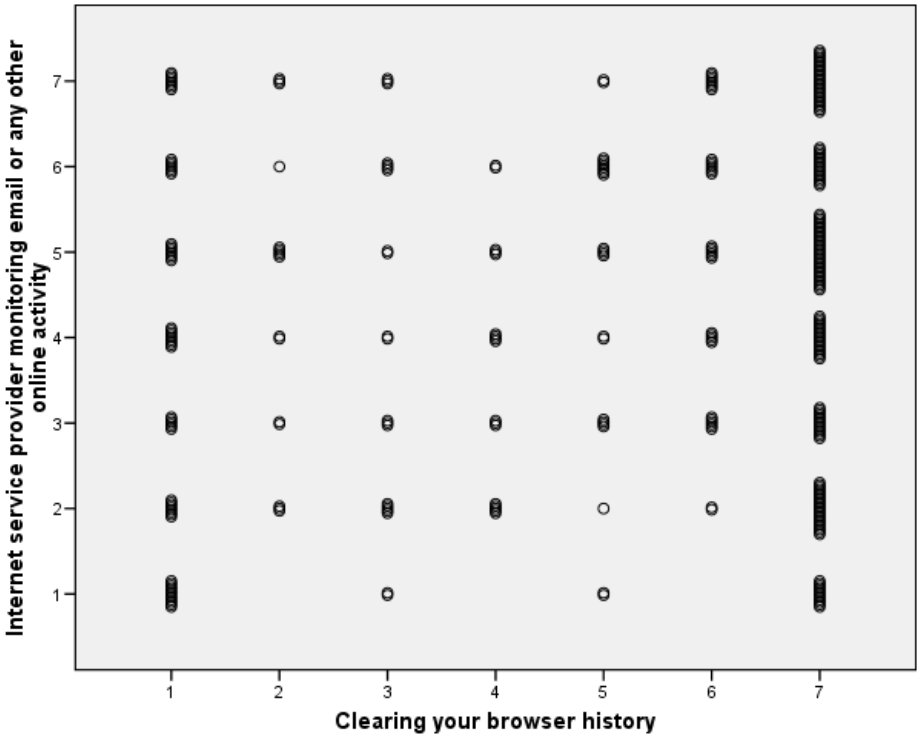

Receiving spam/junk email
1
2
3
4
5
6
7
Use Internet email

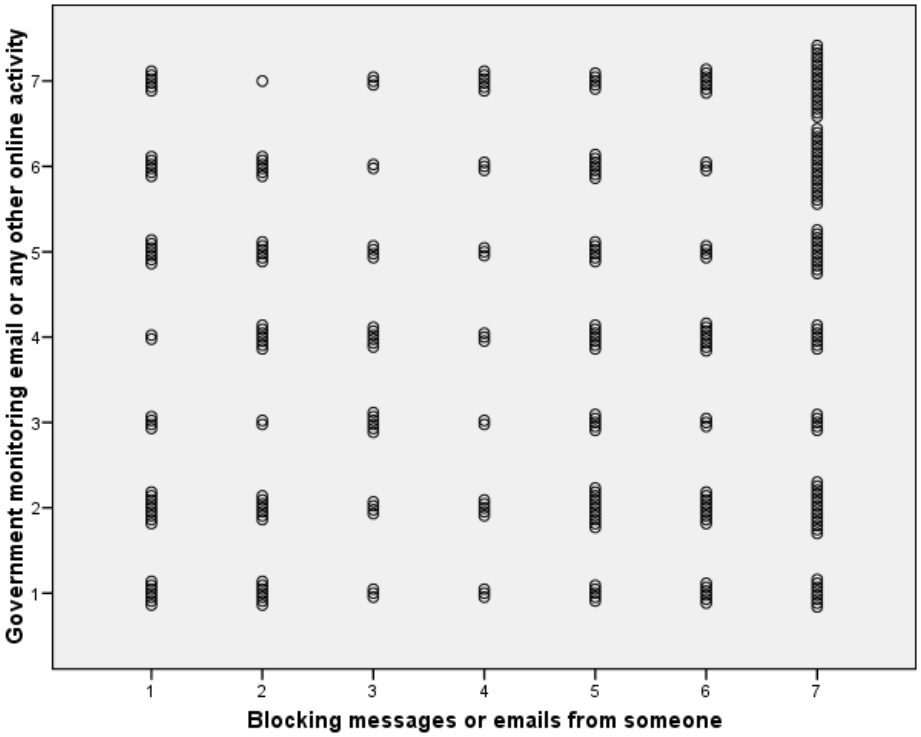

Internet service provider monitoring email or any other online activity
1
2
3
4
5
6
7
Finding a privacy certification on a web site before registering your information

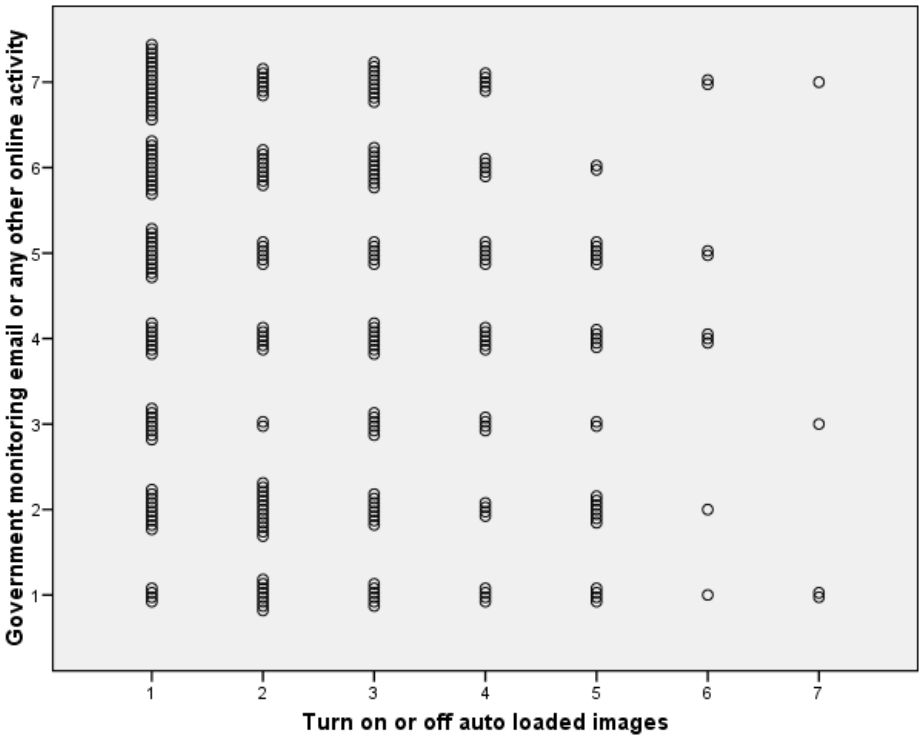

Hacker obtaining personal medical information online
1
2
3
4
5
6
7
Use advanced search techniques with a search engine

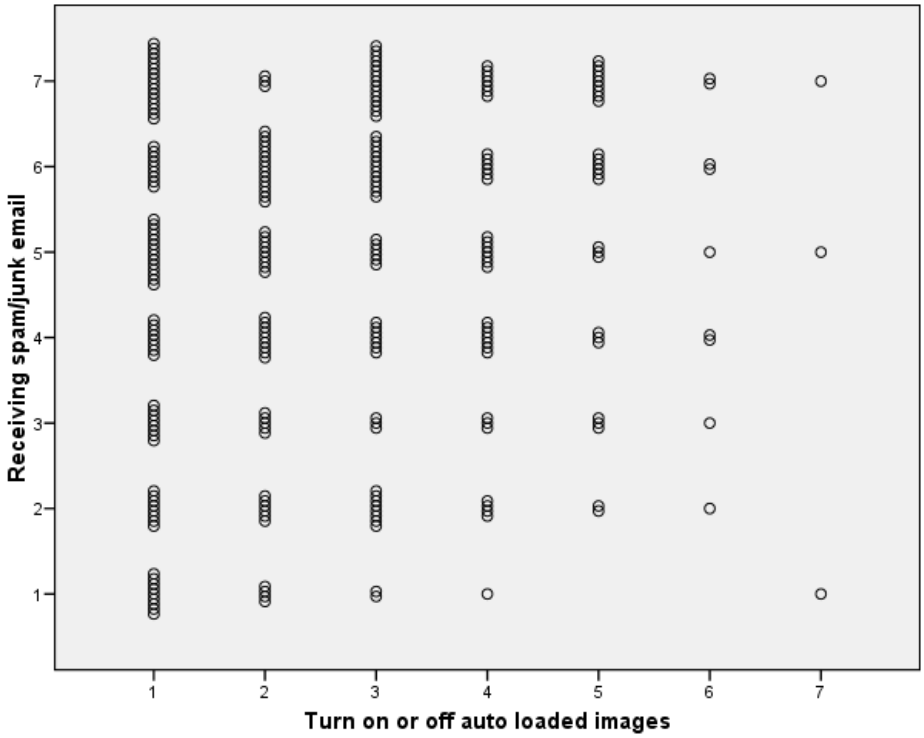

Attack of a computer virus
1
2
3
4
5
6
7
Changing cookie preferences

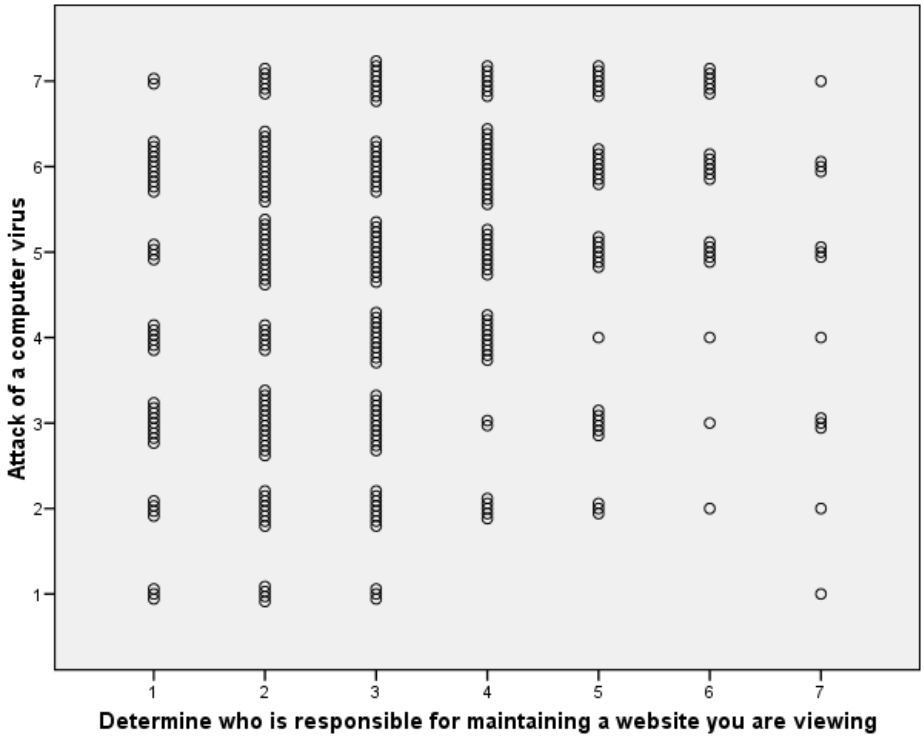

Hacker obtaining personal medical information online
1
2
3
4
5
6
7
Chatting online

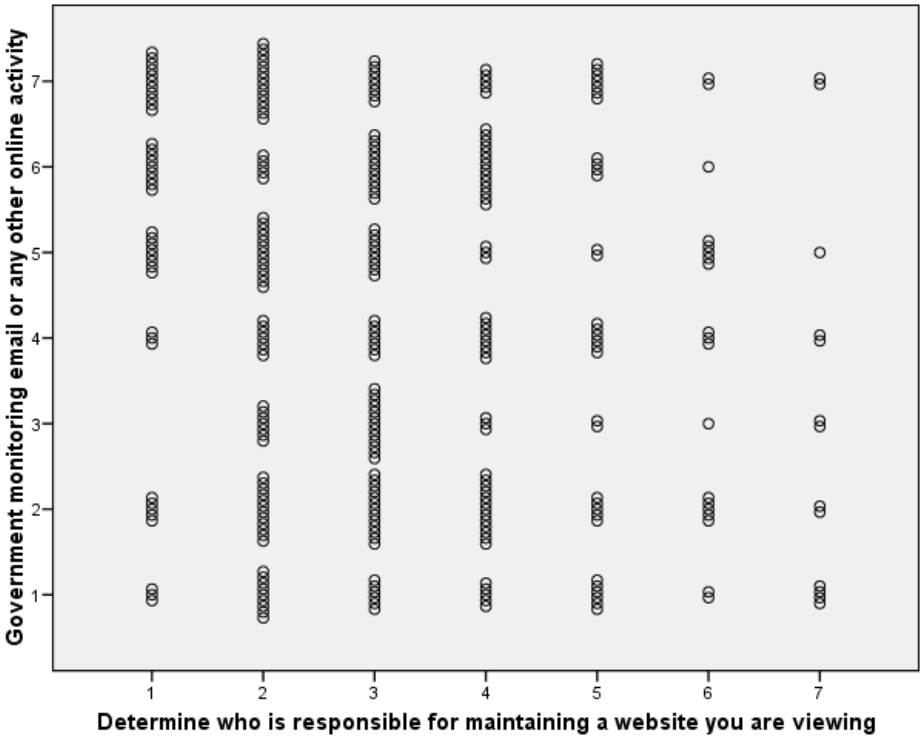

Internet service provider monitoring email or any other online activity
1
2
3
4
5
6
7
Clearing your browser history

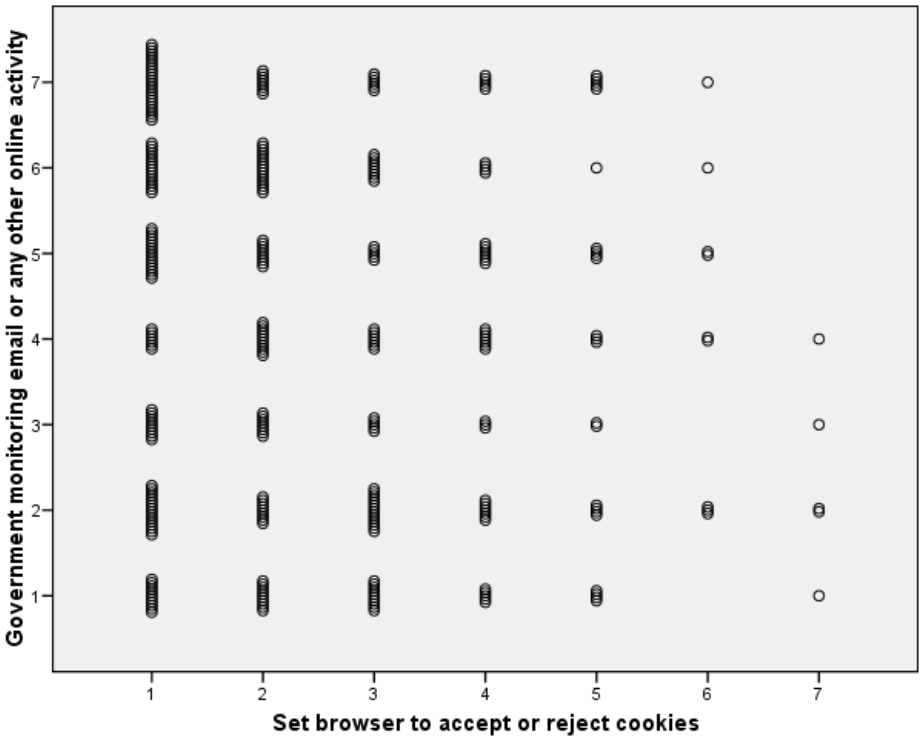

Government monitoring email or any other online activity
1
2
3
4
5
6
7
Blocking messages or emails from someone

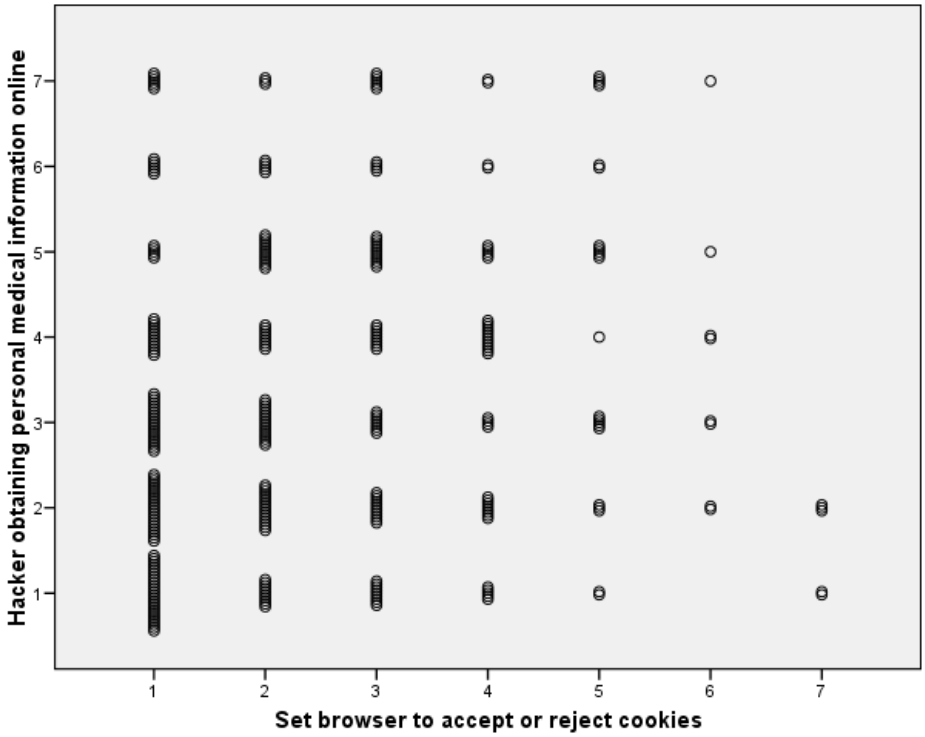

Government monitoring email or any other online activity
1
2
3
4
5
6
7
Turn on or off auto loaded images

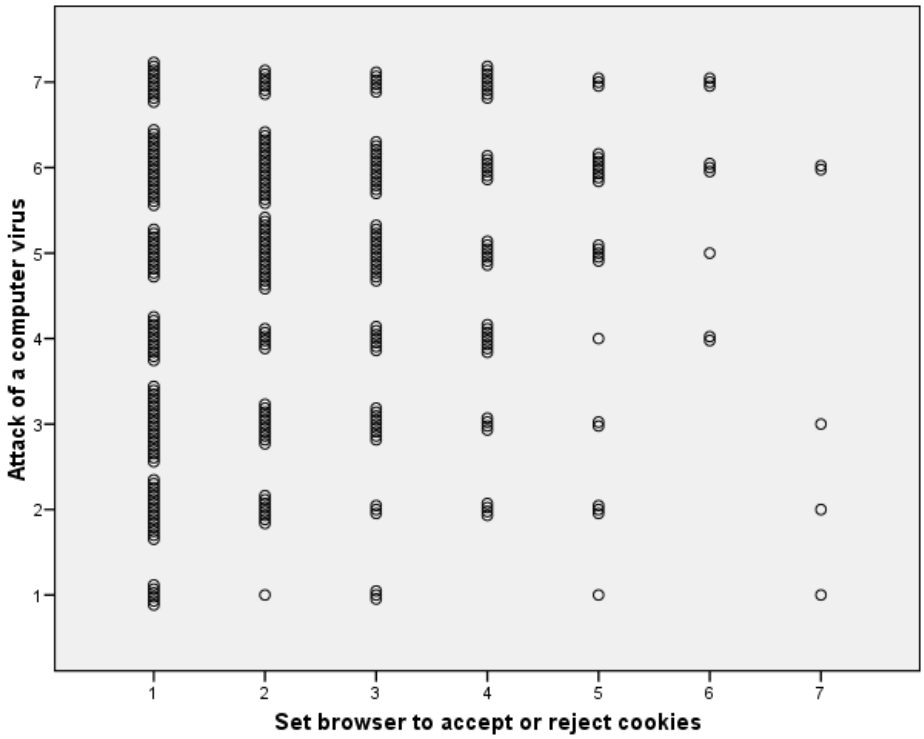

Receiving spam/junk email
1
2
3
4
5
6
7
1
2
3
4
5
6
7
Turn on or off auto loaded images

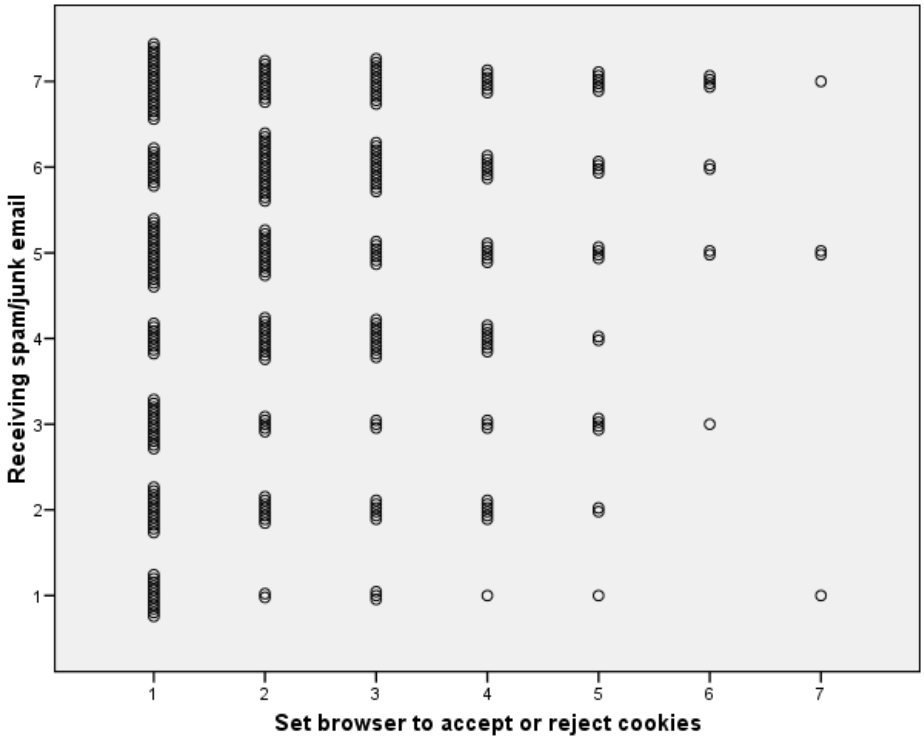

Attack of a computer virus
1
2
3
4
5
6
7
1
2
3
4
5
6
7
Determine who is responsible for maintaining a website you are viewing

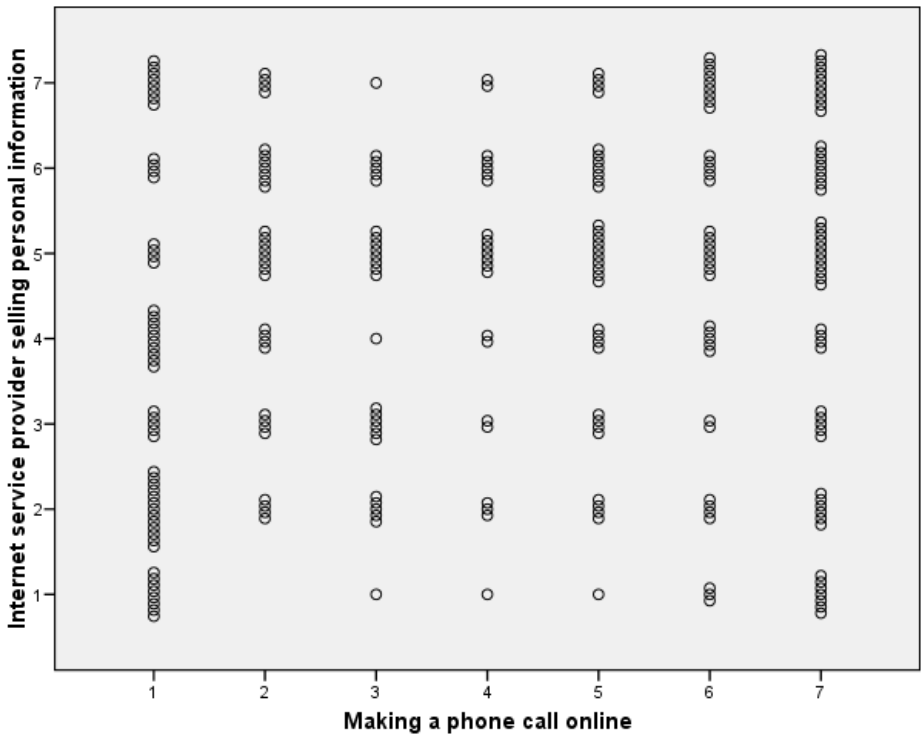

Government monitoring email or any other online activity
1
2
3
4
5
6
7
Determine who is responsible for maintaining a website you are viewing

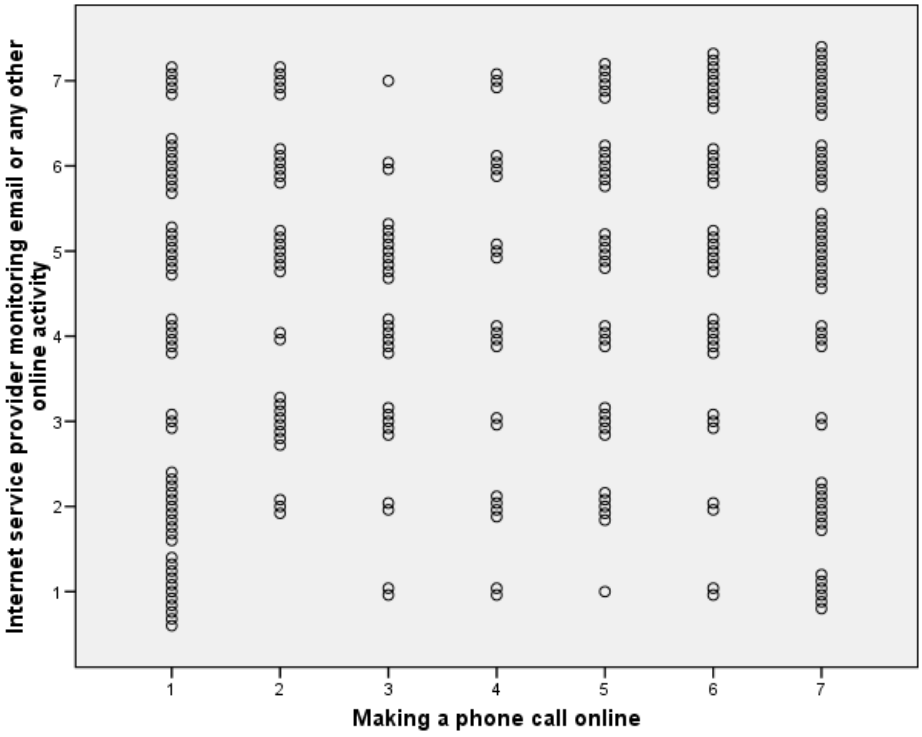

Government monitoring email or any other online activity
1
2
3
4
5
6
7
Set browser to accept or reject cookies

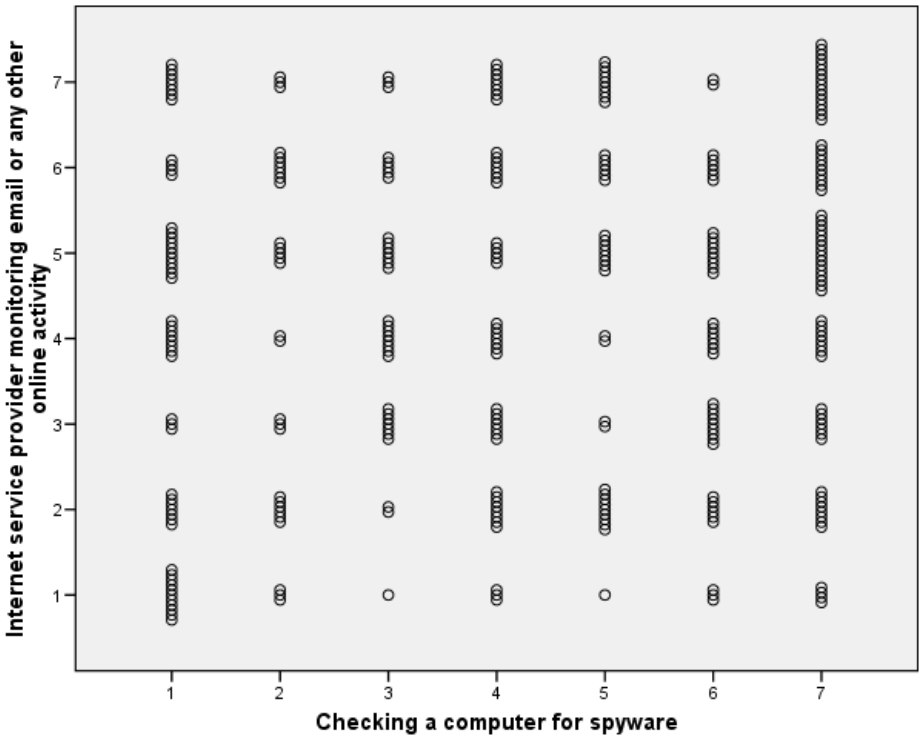

Hacker obtaining personal medical information online
1
2
3
4
5
6
7
1
2
3
4
5
6
7
Set browser to accept or reject cookies

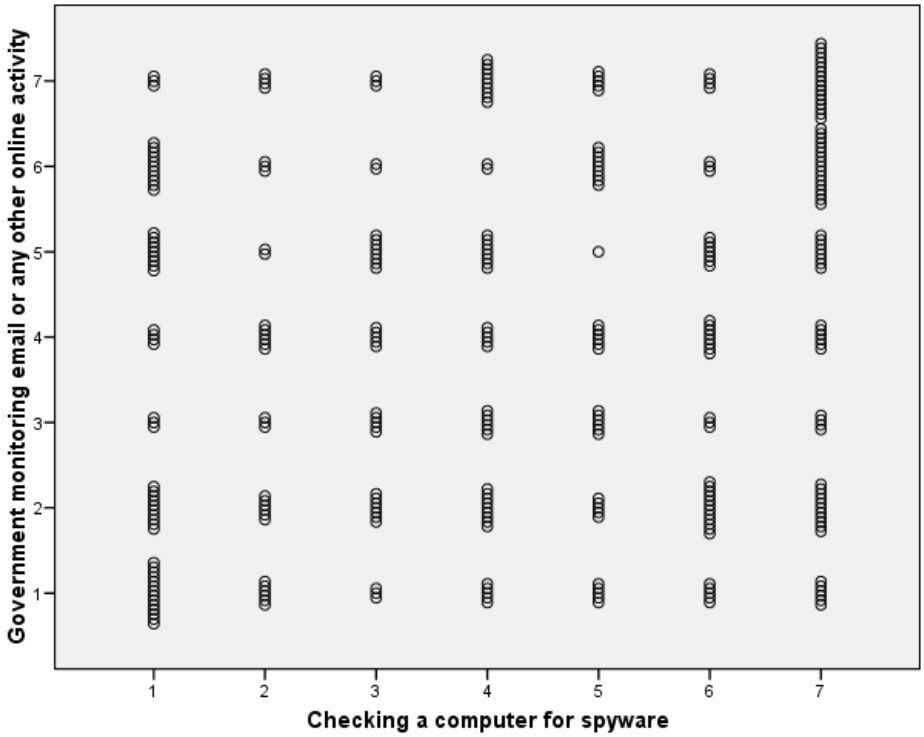

Attack of a computer virus
1
2
3
4
5
6
7
1
2
3
4
5
6
7
Set browser to accept or reject cookies

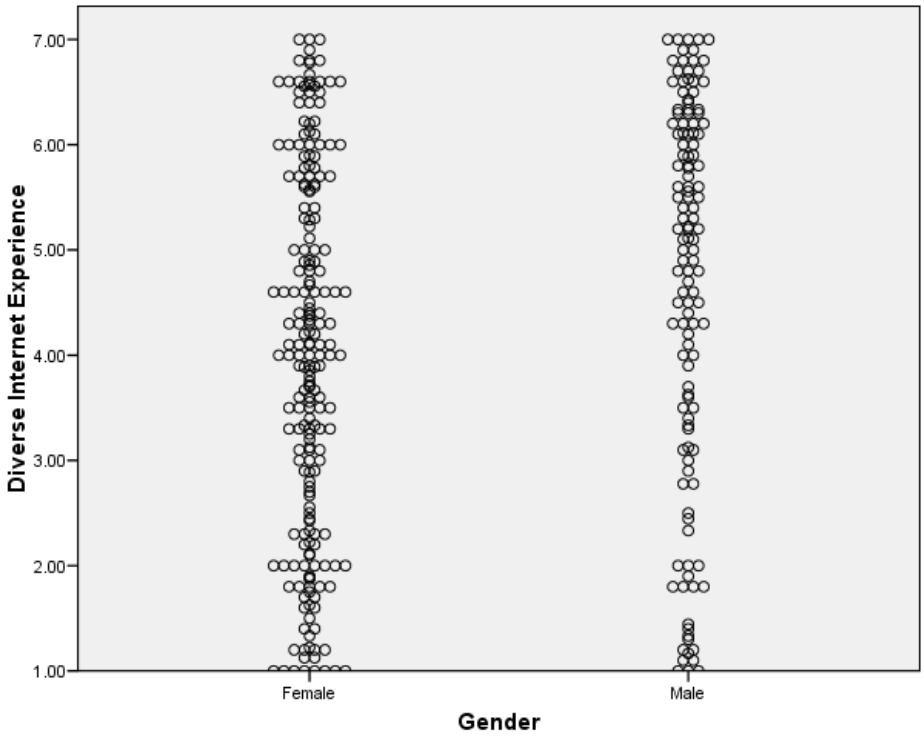

Receiving spam/junk email
1
2
3
4
5
6
7
1
2
3
4
5
6
7
Set browser to accept or reject cookies

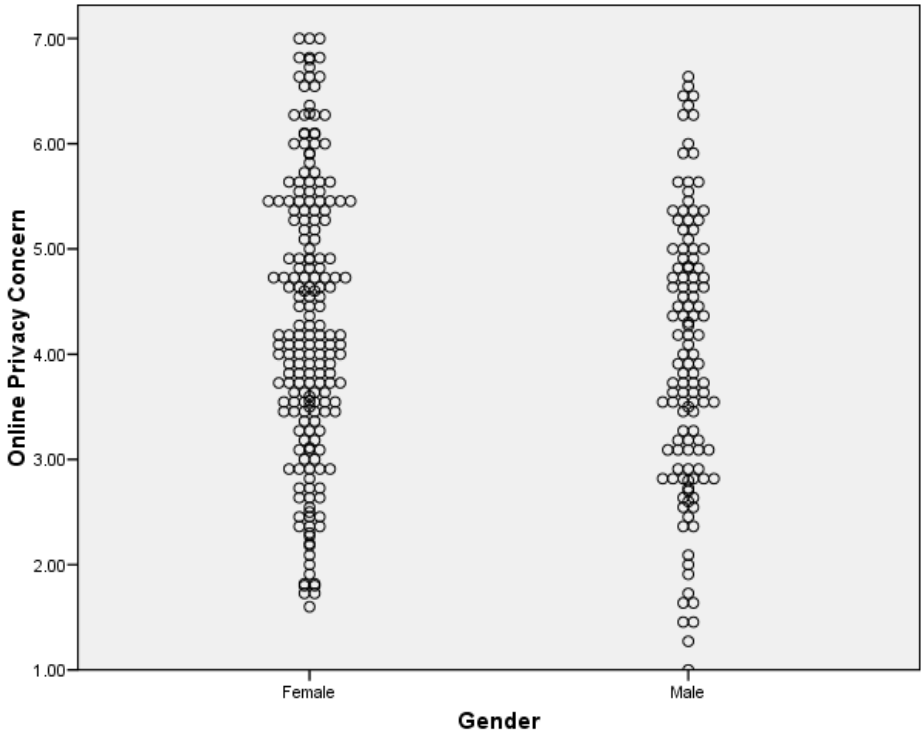

Internet service provider selling personal information
1
2
3
4
5
6
7
1
2
3
4
5
6
7
Making a phone call online


Internet service provider monitoring email or any other online activity
1
2
3
4
5
6
7
Making a phone call online


Internet service provider monitoring email or any other online activity
1
2
3
4
5
6
7
Checking a computer for spyware


Government monitoring email or any other online activity
1
2
3
4
5
6
7
Checking a computer for spyware


Diverse Internet Experience
7.00
6.00
5.00
4.00
3.00
2.00
1.00
Female
Male
Gender


Online Privacy Concern
7.00
6.00
5.00
4.00
3.00
2.00
1.00
Female
Male
Gender